IBM WebSphere Host On-Demand Version 6.0

Getting Started

IBM WebSphere Host On-Demand Version 6.0

Getting Started

Note
Before using this information and the product it supports, read the information in "Appendix E. Notices" on page 79.

Third Edition (September 2001)

This edition applies to Version 6.0 of IBM® WebSphere Host On-Demand (program number 5733-A59) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this book

This book helps you install Host On-Demand Version 6 and plan for configuration after installation. Once you install Host On-Demand, you can use the online help to define users and groups, configure clients, and complete other administrative tasks. This book is written for administrators.

This graphic is used to highlight notes to the reader.

This graphic is used to highlight tips for the reader.

Chapter 1. Introducing Host On-Demand

The browser-based access of IBM WebSphere Host On-Demand Version 6 (Host On-Demand) gives you a simple way to reach critical host data, without requiring you to install any software on your workstation. Host On-Demand uses the power of Java technology to open the doors to your host system whenever you need it, wherever you need it, directly from your browser. Just click on a hyperlink to launch the Host On-Demand Java applet. This Web-to-host connectivity solution provides secure Web-browser access to host applications and system data through Java-based emulation, so you can take existing host applications to the Web without programming.

Support for TN3270E, TN5250E, VT420 and IBM CICS Gateway for Java access provides a single interface to key host data. Because Host On-Demand is Java-based, its interface has the same look-and-feel across various types of operating environments. Host On-Demand also provides a default graphical user interface (GUI) to simplify the experience for users who are unfamiliar with traditional ″green screens.″

Using Secure Sockets Layer (SSL) Version 3.0, Host On-Demand extends secure host data access across intranets, extranets, and the Internet. Mobile workers access a secure Web site, receive authentication and establish communication with a secure enterprise host. With client and server certificate support, Host On-Demand can present a digital certificate (X.509, Version 3) to the Telnet server - such as IBM Communications Server for Windows NT Version 6 or later, or IBM Communications Server for OS/390 Version 2.6 or later - for authentication. Host On-Demand can also integrate the SSL client authentication with IBM Vault Registry. This allows you to benefit from industry standard public key infrastructure (PKI) methods. Users request a certificate from IBM SecureWay Vault Registry, which manages, maintains and ensures certificate validity.

Database On-Demand is included with Host On-Demand to provide access to DB2 information stored on iSeries computers using a Java Database Connectivity (JDBC) driver. Database On-Demand is a Java applet that allows you to perform Structured Query Language (SQL) requests to iSeries databases through a JDBC driver.

Host On-Demand is multilingual and is available in 23 languages, including double-byte character set languages. Support for the European currency symbol, as well as keyboard and code-page support for many more languages such as Arabic, Hebrew and Thai, is also provided. All language versions are available on the same media, and multiple language versions can be accessed concurrently.

Host On-Demand is shipped on four CDs: one for the OS/400; one for AIX and other UNIX platforms; one for multiple platforms, including Windows, OS/2, and Novell; and one for the Host Access Toolkit. It is also available on tape as a zSeries (TM) program product.

For up-to-date information, go to the Host On-Demand Web site at `http://www.ibm.com/software/webservers/hostondemand`.

For the latest technical hints and tips for Host On-Demand, go to the `Host On-Demand Hints and Tips site`.

To subscribe to the Software Support Bulletin, go to http://www.ibm.com/software/network/support.

Why use Host On-Demand?

There are a number of reasons to use Host On-Demand:

A cost-effective approach

You can save money in product deployment and maintenance by installing Host On-Demand on a Web server, eliminating the need to manage individual user desktops. Users can connect directly to a host system, such as an IBM iSeries system or an IBM zSeries system, eliminating the need for extra hardware and software required by connecting back through the Web server. Host On-Demand can be installed on nearly any server platform, accommodating various size organizations and branch offices.

Host On-Demand uses a Java applet, which helps to reduce your software maintenance costs and allows easy management of configuration data. Since the applets reside on a server and are downloaded to Web browsers when needed, you no longer have to schedule maintenance and upgrades. Upgrade the software on the server and users receive the upgrade the next time they request the applet. You can control the rate of this upgrade as needed. And server maintenance is less complex with Web-based remote configuration and administration.

Host On-Demand includes a deployment wizard, which enables you to create custom HTML pages. These pages can tailor the content and function of sessions to meet the needs of specific groups of users.

Create new e-business applications

Host On-Demand provides a rich tool set to deliver custom e-business applications that meet your specific business needs. These tools include the Host Access Class Library API, Host Access Beans for Java and ActiveX controls.

The Host Access Class Library API provides access to 3270, 5250 and VT data streams. These class libraries allow you to use mission-critical information in new ways, such as integrating data from one application into another.

Host Access Beans for Java provides host connectivity and emulator functions through simple, component-based development tools, like IBM Visual Age for Java. You can use these beans to rapidly create custom applications that allow you to deliver the specific functions you want to include in your host access applications. These object oriented beans help you minimize development efforts through software reuse. Application developers who are familiar with ActiveX can use IBM Host Access Controls - a set of ActiveX controls used to provide the functionality found in Host Access Beans for Java.

The Host On-Demand J2EE Connector provides host connectivity functions for use on a J2EE-compatible Web application server such as the WebSphere Application Server Enterprise Edition.

Connect directly to any Telnet server

Emulation function is contained in the client applet, eliminating the need for a middle tier server as part of the connection to the host system, which is both a performance and security issue. Once the applet is served to the client, it is easy to

connect directly to any standard Telnet server that provides the best access to the required data. The Telnet connection can be changed as often as your requirements for new data change. Because no middle-tier server is required, there is no additional capacity needed on your Web server.

Simple management of configuration data

Host On-Demand provides a flexible set of management options for controlling its operation.

For companies that already have user groups defined, administrators can deploy Host On-Demand without recreating user groups. Group-level configuration data (session configuration, macros, keyboard, color mapping, etc.) is defined centrally while user-specific data is stored on users' machines.

For companies that do not have user groups defined, or that need to centrally manage user-specific configuration data, administrators can define users on the Host On-Demand server. Both group-level and user-specific configuration data is defined on the server and can be managed and shared from this server.

As an alternative to the built-in Host On-Demand private data store, you can use an LDAP server to store Host On-Demand configuration information. This includes LDAP storage of all user, group and session configuration information, like keyboard mappings, macro definitions, and session parameters. A migration facility is also provided to migrate existing Host On-Demand profiles into LDAP.

Windows integration

Host On-Demand provides two features for Windows users. First, users can print in the same manner as other desktop Windows applications. Second, if you are using defined users on the Host On-Demand server, these user IDs can be the same as your Windows domain user IDs, which are retrieved directly from the operating system and defined automatically. If this feature is enabled, users who log on to their Windows domain user IDs are not required to log in again to access their Host On-Demand sessions.

What's new in Version 6.0

The following functions and enhancements were added to Host On-Demand Version 6.0:

More flexibility and control over locally stored user preferences

You can define centrally stored session-configuration preferences while also allowing users to maintain individual preferences. Users are able to run sessions using the default configuration you define, and users can further modify sessions according to personal preference. These personalized changes are stored on users' local machines separate from any default session configuration information. When you change the default configuration, users receive those updates automatically without losing any personalized changes.

Deployment Wizard enhancements

The Deployment Wizard helps you create HTML pages more easily to give your users better host access. This will help you determine a deployment strategy for your users. Additionally, new configuration models have been added to specify how Host On-Demand sessions are defined and managed. See deployment wizard

in the Host On-Demand online help for more information. Streamlined panel flow and other usability improvements to the Deployment Wizard panels make administration easier. Online help for the Deployment Wizard is now available from within the Wizard panels.

Native Windows print support

Windows users can print using the standard printer drivers. Users can use their default Windows printers without additional configuration, and they can change properties without closing their host printer sessions.

Integrated Windows domain logon

If this function is enabled, users are not required to log on to the Host On-Demand server to access their configuration data. Host On-Demand retrieves the Windows domain user ID, which becomes the Host On-Demand user name. If a user is already defined on the server, the configuration data for that user is accessed. Otherwise, new users are automatically created with group default settings. You can use the Deployment wizard to configure this function (see the online help for instructions).

Customizable toolbar

Administrators and users can customize the toolbar buttons used for Host On-Demand sessions. Users can add and edit toolbar buttons to launch an applet, run an application, go to a URL, run a macro, or perform a menu function. After customizing the toolbar, settings are saved for future sessions.

Cached client support across the Internet

Host On-Demand keeps the cached components at a consistent level and prevents users from installing different and potentially conflicting versions of components from different servers. Clients can communicate with servers running different levels of Host On-Demand.

Support for Java2-enabled browsers

Clients are supported on Java2-enabled Web browsers, such as Netscape 6.x and Mozilla. The Java2 plug-in with Netscape 4.x and Microsoft Internet Explorer is also supported.

JVM 1.3 support on server

Host On-Demand supports JVM 1.3 on the server.

Tab to next word and delete word

Similar to Personal Communications emulation, users or administrators can move the cursor easily between words or delete a word using supported function keys. Supported function keys can be defined as Tab Word, Backtab Word, Next Word, Previous Word, and Delete Word.

Problem determination enhancements

A customer support person can activate and control the Host On-Demand trace facility for an emulator client session by specifying parameters in the associated HTML file. You can also add an optional parameter that launches the IP monitor utility on a Host On-Demand emulator session. A troubleshooting section is added to the online help table of contents so that you can troubleshoot common problems before calling IBM Service.

Copying sessions more easily

Users can create new sessions easily by right-clicking an existing session and selecting Copy. Administrators can create new sessions easily by right-clicking an existing session and selecting Duplicate Session. Administrators can also copy and paste existing sessions into other user and group definitions using the right-click menu.

User-defined character mapping editor for double-byte character set (DBCS) environments

You can use customized user-defined character (UDC) mapping in your session (3270, 5250, 3270 host print) instead of default mapping. You can create a UDC translation table using the UDC mapping editor to store customized mapping for your session.

Basic support for GB18030

Chinese characters can be processed with GB18030 code-page support (extended EBCDIC support only).

Chapter 2. Planning for Host On-Demand

- Deployment strategy considerations
- Before installing Host On-Demand
- Supported server operating systems
- Supported client operating systems
- Disk space requirements
- Supported browsers
- Packaging

Deployment strategy considerations

Host On-Demand provides access to host applications from a Web browser. The browser downloads the Host On-Demand Java applet from the Web server (flow A) and then connects to any Telnet server to access host applications (flow C). The configuration servlet is part of the Web server. The Host On-Demand applet needs configuration information to determine which host to connect to and other host session properties. This configuration information can be provided to the Host On-Demand applet from an HTML file or using the Host On-Demand configuration server.

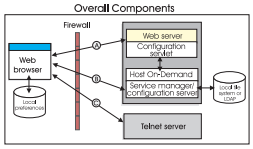


Figure 1. How Host On-Demand Components Integrate with Other Components

Understanding the HTML-based model

You can use the Deployment Wizard to create HTML files that contain configuration information for host sessions. Therefore, you are not required to use the Host On-Demand configuration server to specify sessions. If you allow users to save changes to the host session configuration information, their changes are stored on the local file system where the browser is running. This option of defining configuration information is called the HTML-based model.

Understanding the configuration server-based model

In the configuration server-based model, host session information is maintained on the configuration server using the administration utility, and the information is defined using a user and group structure. The configuration server normally stores its data locally on the Host On-Demand server machine, though it can be configured to use LDAP instead. Users access their configurations using either custom HTML files created in the Deployment Wizard or by using one of several HTML files that are provided as part of Host On-Demand. Each user has a unique user ID defined in the configuration server, and in most cases the user needs to log on to the Host On-Demand server before viewing his sessions. If administrators allow users to save changes, user preferences are stored in the configuration server by user ID.

Understanding the combined model

Host On-Demand supports a combined model where the host session information is defined in the configuration server using the administration utility. In the combined model you use the Deployment Wizard to create an HTML file that points to the host session information stored in the configuration server. Users do not see a logon panel, and if you allow users to save changes to the host session configuration information, their preferences are stored on the local file system where the browser is running.

Other deployment considerations

If you use the configuration server and it is separated from your Web browser by a firewall, you will either need to open up the configuration server port on the firewall or run the Host On-Demand configuration servlet. The configuration servlet allows the browser to communicate with the configuration server across standard Web protocols, such as HTTP or HTTPS. See Flow B in the preceding diagram.

If you deploy the cached client to the Internet, consider that your users might use Host On-Demand with other business partners running Host On-Demand servers at different service levels. This could be a problem if your user needs different functions when accessing servers at different service levels. Components of different service levels are not supported within a single cached client, and there can be only one cached client on a machine. Host On-Demand Version 5.0.4 or higher is required to run the cached client across the Internet.

To prevent complications, you can do some or all of the following:

- Select all the functions a user needs (across all sites the user accesses) in a preload list when you create an HTML page using the Deployment Wizard
- Use the disable function of the Deployment Wizard to disable all functions not in the preload list and the functions that are not needed for your users
- Create separate HTML pages for different user groups
- Give your HTML pages a name that identifies your company
- Always install Screen Customizer to prevent users who are accessing your server from losing Screen Customizer functions when accessing other sites

For information about deploying cached clients to the Internet, see Cached client support across the Internet .

Before installing Host On-Demand

Below are some general software requirements and information to help you make configuration decisions before installing Host On-Demand. Check the installation section in this Getting Started guide for specific software requirements for your operating system; read the readme for late breaking information; and read the Basic Configuration Steps for more detailed information about configuring Host On-Demand after installation.

Install a JDK or JVM (on non-Windows platforms), a Web server and, optionally, a servlet engine

Use the installation section in this guide for supported JDK and JVM, browser, Web server and servlet engine levels, as well as required disk space.

Determine directory structure for Host On-Demand installation

The installation instructions, and automated installations, assume a certain

directory structure. In most cases these defaults should work fine. Review the directory structure in the installation section in this guide before installing. If you change the default directory structure, keep your changes in mind when following the installation instructions.

Select the Service Manager port

The default Service Manager port is 8999. If you want to change this value because it is already in use, you may change it during installation for Windows NT, Windows 2000, and AIX. The port may also be changed after installation on all platforms.

Choose to use the configuration servlet

During the Windows NT, Windows 2000, and graphical AIX installations, if the installation program detects a supported application server, you are given the option to use the configuration servlet. The configuration servlet allows client applets to communicate with the configuration server through a firewall without opening any additional ports on the firewall. The configuration servlet can be installed manually on the other operating systems, and for web and application servers that are not recognized by the installation program. See installing the configuration servlet in this guide for more information.

Decide what security levels to set

You can configure your Web server to use SSL (HTTPS), so that the data stream from your Web server to your browser is encrypted. See your Web server documentation for more information about configuring your Web server for SSL. Once the client is loaded in a browser, however, it communicates directly with the host. You may be able to configure Host On-Demand to provide SSL security to your host sessions.

- If the Telnet server supports SSL, the clients can be configured to also use SSL. See your Telnet server's documentation for more information about configuring SSL on the Telnet server, and see security in the Host On-Demand online help for more information about configuring a client to connect to a secure Telnet server.
- If your Telnet server does not support SSL, and you are running Host On-Demand on Windows NT or AIX, you can configure the Host On-Demand Redirector to provide SSL support. The Redirector acts as a transparent proxy between the client and the Telnet server by using port remapping. It can encrypt data between the client and itself, between itself and the host, or both between the client and itself and between itself and the host. See adding a host to the Redirector in the Host On-Demand online help for more information.
- If you want session configuration information to be encrypted, you can configure sessions to use the configuration servlet over HTTPS (after configuring your Web server for SSL) instead of communicating directly with the Service Manager. See installing the configuration servlet in this guide for more information about installing the configuration servlet, and see configuring the configuration servlet in the Host On-Demand online help for more information about configuring clients to use the configuration servlet.

Install and configure Host On-Demand

Follow the installation instructions in this guide to install Host On-Demand 6.0, then see Basic Configuration Steps in the Host On-Demand online help for more detailed information about configuring Host On-Demand so users can access host sessions.

Supported server operating systems

For updates to this information, refer to the readme file.

A Host On-Demand server can be installed on the following operating systems:

- Windows NT 4.0 with SP5 or later
- Windows 2000 (Professional, Server and Advanced Server)
- AIX (R) Version 4.3.3, 4.3.4, and 5.1
- OS/2 (R) Warp Server Version 4 and OS/2 Warp Server for e-Business 4.5
- Novell NetWare Version 4, 5, and 6
- Sun Solaris 2.6, 2.7, and 2.8
- OS/400 (R) Version 4 Release 4, Version 4 Release 5, and Version 5 Release 1
- HP-UX 10.20 and 11.00
- Red Hat Linux 6.2, 7.0, and 7.1
- SUSE 6.4, 7.0, and 7.1
- OS/390 Version 2 Releases 5, 6, 7, 8, 9, 10, 11, and 12 (for Version 2 Release 10, you must update JVM 1.1.8 with PTF 6)
- Caldera 2.3
- TurboLinux 6.0 and 6.1
- Unixware 7
- Linux on S/390

Supported client operating systems

For updates to this information, refer to the readme file.

A Host On-Demand client can be installed on the following operating systems:

- Windows 95
- Windows 98
- Windows Millennium Edition (ME)
- Windows NT 4.0 with SP5 or later
- Windows 2000 (Professional)
- AIX 4.3.3, 4.3.4, and 5.1
- OS/2 Warp 4
- Sun Solaris 2.6, 7, and 8
- HP-UX 10.20 and 11.00
- Red Hat 6.2, 7.0, and 7.1
- SUSE 6.4, 7.0, and 7.1
- Caldera 2.3
- TurboLinux 6.0 and 6.1
- Windows Terminal Server Version 4
- Windows 2000 Terminal Services
- Netstation V2R1M0

Disk space requirements

These requirements are based on a typical installation and are only estimates. Sizes can vary by operating system and which languages are installed.

- Windows NT or Windows 2000 - 174MB (English only. Add 4 to 8MB for each additional language)
- AIX (installp image) - 124MB (English only. Add 4 to 8MB for each additional language. Includes the additional security files)
- UNIX (Solaris, HP-UX or Linux) - 110MB (English only. Add 4 to 8MB for each additional language)
- iSeries - 230MB DASD
- OS/2 and Novell - 230MB

Supported browsers

Browsers are dynamic. For the most up-to-date information, refer to the readme file and to the Host On-Demand Web site. The following browsers are supported for you to download the Host On-Demand clients from a remote Host On-Demand server or to run Host On-Demand on a locally installed client:

- Netscape Navigator 4.6, 4.7, and 6.0
- Netscape Navigator (OS/2) 4.61 and IBM Mozilla Web Browser for OS/2
- Microsoft Internet Explorer 4.01 (with SP1), 5.0, 5.1, 5.5, and 6.0
- Other browsers that support the JRE 1.3 plug-in

Packaging

Host On-Demand is provided on four CDs: one CD for multiple platforms, including Windows, OS/2, and Novell; one CD for AIX and other UNIX platforms, including HP-UX, Linux, and Solaris; one CD for OS/400; and one for the Host Access Toolkit. Each CD includes the code, publications, help files, and other files for all the supported languages.

Installation formats provided on the CDs include:

- InstallShield for Windows NT, Windows 95, Windows 98, and Windows 2000
- ZIP for OS/2 and NetWare
- installp for AIX
- TAR for Linux, Solaris, and HP-UX
- Separate CD for OS/400
- Separate CD for the toolkit

For z/OS, Host On-Demand is provided on three different media:

- 6250 tape
- 3480 cartridge
- 4 millimeter cartridge

Chapter 3. Installing Host On-Demand

The Host On-Demand clients are served as Web pages, so you must install the Host On-Demand server in the same environment as a Web server.

After installing Host On-Demand Version 6 on a machine running Microsoft Personal Web Server, the virtual directory for Host On-Demand does not show up in the list of virtual directories in the Personal Web Manager GUI. Therefore, after the installation is complete, do not restart the Web server using the Start/Stop button in the Personal Web Manager GUI. Instead, restart the Web server using the Services GUI in Windows. You can also manually add the directory to the list of virtual directories in the Personal Web Manager GUI.

Installing the Host On-Demand server

The installation steps are different for each operating system.

- Installing on Windows NT or Windows 2000
- Installing on OS/2
- Installing on Novell NetWare
- Installing on AIX
- Installing on UNIX
- Installing on OS/400
- Installing on z/OS

Installing on Windows NT and Windows 2000

A Windows NT Web server is required to install Host On-Demand on Windows NT or Windows 2000. The following Web servers are recognized and automatically configured:

- IBM Internet Connection Server
- Microsoft Web Servers:

Internet Information Server 3 and 4
Peer Web Services
Personal Web Server

- Lotus Go, Domino, and Domino Go
- IBM HTTP Server
- Netscape Enterprise Server

You can install Host On-Demand with a graphical interface using the Windows InstallShield or with a response file using Windows InstallShield in silent mode.

Installing Host On-Demand using InstallShield

To automatically install Host On-Demand on a Windows NT or Windows 2000 workstation using InstallShield, follow the steps below.

You must be a member of the Administrators group.

1. If CD autoplay is enabled on your Windows NT or Windows 2000 server, insert the CD and wait for the start window. Otherwise, insert the CD and run the `setupwin.exe` program in the root directory.
2. Click Install Product.
3. Follow the directions in the installation windows.
   - The default server directory is `hostondemand` . If you are upgrading, the installation program uses the same server directory as before. The server directory contains files used only by the server and must not be available to client workstations.
   - The default publish directory is `\hostondemand\HOD`. The publish directory contains files that must be available to client users who access the server through a browser.
   - The default Service Manager port is 8999, and it is usually a safe port to select. Check your server documentation to see if this port is being used. If it is in use, you can change the port during installation, or later. For more information about changing the Service Manager port, see Changing the Service Manger's configuration port in the online help.
   - If the installation program detects IBM WebSphere Application Server, Lotus Domino Go Web Server or IBM Domino Go Web Server installed, you are asked if you want to use the configuration servlet to connect to the configuration server for client configuration information. If you are running Host On-Demand through a firewall, this eliminates the need to open an extra port for the configuration server. Answering Yes automatically configures the clients to access the configuration server through the configuration servlet. Answering No configures the clients to access the configuration server directly on port 8999, which was the default configuration for Host On-Demand Version 4. See installing the configuration servlet in this guide for more information.
4. If you have not already done so, read the readme file (available in the last window after installation).
5. If a message tells you that your Web server is not recognized or was not configured, configure it. If you install a Web server later or your Web server is not recognized by Setup, you must publish the Publish directory to the Web. Refer to the Web server documentation for information on how to publish the directory.
6. Restart the Web server.
7. Load the `HODMain.html` , located in the `hostondemand\HOD` directory, into your browser. This page contains links to all the Host On-Demand clients, the readme file, and basic configuration steps for configuring the Host On-Demand server.
8. Click Start > Programs > IBM Host On-Demand > Administration > Getting Started.

At the end of installation, the Host On-Demand Service Manager is started automatically.

Installing Host On-Demand in silent mode

A silent installation installs Host On-Demand without displaying any windows or asking for input. All of the input required during an installation is obtained from a text file called a response file. A response file is created by recording an installation. A local client cannot be installed silently.

When you install in silent mode, there is no indication that installation is in progress or that it is complete.

To record a response file:

```
setup.exe -r -f1d:\temp\server1.iss
```

To install in silent mode:

```
setup.exe -s -f1d:\temp\server1.iss -f2d:\temp\server1.log
```

Options supported in silent mode

-r	Records a response file
-s	Runs a response file and installs Host On-Demand
-f1[path\response_file_name].iss	Defines the response file, in both record and run modes. The path and filename must be 43 characters or fewer. There must not be a space between parameter and value. The filename extension **must** be `iss` .
-f2[path\log_file_name]	Defines the log file and can be used in run mode to create a file that contains a history of an installation. The path and filename must be 43 characters or fewer. There must not be a space between parameter and value.

The target system's configuration **must** be the same as that of the source system (the system on which the response file was created). For example, if the source system has a previous installation of Host On-Demand 6.0, the target system must have the same. If the source system installed Host On-Demand on the D drive, the target system must also have a D drive. The source and target systems must have the same number of Web servers, although they do not need to be the same types.

Format of the silent mode installation log file

If an installation is not successful, the log file might indicate the reason. The format of a log file is as follows:

```
[InstallShield Silent]
Version=v6.00.000
File=Log File
[Application]
Name=\Host On-Demand Server
Version=6.00.000
Company=IBM
[ResponseResult]
ResultCode=0
```

Result code values

The ResultCode indicates whether or not the installation was successful. Possible values are:

-0	Successful

-1	General error
-2	Mode not valid
-3	Required data not found in the response file
-4	Not enough memory available
-5	File does not exist
-6	Cannot write to the response file
-7	Cannot write to the log file
-8	Path to the response file is not valid
-9	Not a valid list type (string or number)
-10	Data type is not valid
-11	Unknown error during setup
-12	Dialogs are out of order. Since the dialog order depends on what other related products were already installed on the workstation, the target system must have the same products.
-51	Cannot create the specified folder
-52	Cannot access the specified file or folder
-53	Selected option is not valid

Common problems:

- The `setup.iss` file is not in the directory specified by the -f1 option.
- You changed the name or location of the `setup.iss` file and did not specify the new name or location when you ran the `setup.exe` command to install the product.
- There is not enough space on specified target drive to install the product.
- You are installing or uninstalling Host On-Demand and you are not logged on to the target machine with Administrator authority.
- There is an error in the syntax of the `setup.exe` command.

Installing on OS/2

The following are required to install Host On-Demand on an OS/2 server:

- Hard disk configured for HPFS
- OS/2 Web server, such as Lotus Domino Go Webserver for OS/2
- OS/2 JVM 1.1.8 or JVM 1.3. You can obtain the latest JVM level from one of the following sites:

  ```
  ftp://ftp.hursley.ibm.com/pub/java/
  http://www.ibm.com/java
  ```

  For JVM 1.1.8, make sure your classpath entry in `config.sys` is updated with the location of the JVM class files and that the current directory (.) is included. The classpath should include something like this:

  ```
  c:\Java11\lib\classes.zip;
  ```

  When you have installed the JDK and set the classpath, reboot the workstation so that the updated classpath takes effect.

If you have previously installed Host On-Demand and have changed /hostondemand/lib/NSMprop or changed or created /hostondemand/hod/config.properties , you must back up these files before installation, then restore them after installation. The files are overwritten during the unzip process.

The following steps assume that hostondemand is the server directory and HOD is the publish directory. To install the Host On-Demand server:

1. Insert the CD.
2. Create a server directory, for example, hostondemand . The server directory contains files that are used only by the server and must not be available to client workstations.
3. Change to the server directory.
4. Run the following command to extract the files:

   ```
   unzip [cd_rom]:\zip\hod60srv.zip
   ```

   where:

   - *unzip* is your unpacking program (such as UNZIP.EXE). It must support long filenames
   - *[cd_rom]* is the CD-ROM drive letter
   - *ZIP* is the directory on the CD
5. Create the publish directory; for example, HOD. The publish directory contains files that must be available to client users who access the server through a browser.
6. Change to the publish directory.
7. Run the following command to extract the files:

   ```
   unzip [cd_rom]:\zip\hod60www.zip
   ```
8. Make the publish directory available to clients on the network. Refer to your Web server documentation for information on how to do that.
9. Configure a local host by adding the following line to the setup.cmd file, which is usually found in the \mptn\bin directory:

   ```
   ifconfig lo 127.0.0.1
   ```
10. Start the Host On-Demand Service Manager, which provides support services for Host On-Demand and runs as a Java application:
    a. At the command prompt, change directory to \hostondemand\lib .
    b. Copy NCServiceManager-OS2.cmd from the \hostondemand\lib\samples\CommandFiles directory.
    c. Edit NCServiceManager-OS2.cmd to reflect the directory paths appropriate for your workstation.
    d. Run NCServiceManager-OS2.cmd. The Service Manager does not display a message indicating that it has started.

For Host On-Demand to function, the Service Manager must be running. If you reboot the server, you must also restart the Service Manager. You might want to add the command to your startup.cmd file so that the Service Manager starts automatically when the workstation boots. If you do, remember to include logic to change directory to the \hostondemand\lib subdirectory before the command runs.

11. Restart the Web server.

12. Load HODMain.html , located in the \hostondemand\HOD directory, into your browser.
    - Click readme to see updated information.
    - Click Basic configuration steps to help you get started with configuring the Host On-Demand server.

Installing on Novell NetWare

The following are required to install Host On-Demand on a Novell server:

- Novell NetWare 4.*x*
- Novell Web Server
- Novell Java Development Kit 1.1.8

To obtain the Novell JDK, go to http:\\www.developer.novell.com. The JDK must be configured for long-filename support.

If you have previously installed Host On-Demand and have changed /hostondemand/lib/NSMprop or changed or created /hostondemand/hod/config.properties , you must back up these files before installation, then restore them after installation. The files are overwritten during the unzip process.

These steps assume that hostondemand is the server directory and HOD is the publish directory. To install the Host On-Demand server:

1. From a client workstation, map a drive to the SYS: volume of the Novell server.
2. Mount the SYS: volume.
3. Insert the CD.
4. Create a server directory; for example, hostondemand. The server directory contains files that are only used by the server and must not be available to client workstations.
5. Change to the server directory.
6. From the drive mapped to the SYS: volume, run the following command to extract the files:

   ```
   unzip [cd_rom]:\zip\hod60srv.zip
   ```

   where:
   - *unzip* is your unpacking program (such as UNZIP.EXE). It must support long filenames.
   - *[cd_rom]* is the CD-ROM drive letter.
   - *zip* is the directory on the CD.
7. Change to SYS:\web\docs. This directory is usually published (made available to client users who access the server through a browser) automatically. If the \web\docs directory does not exist, create a publish directory, for example HOD , change to that directory, and go to Step 10.
8. Create a directory named HOD and change to that directory. The HOD directory contains files that must be available to client users who access the Host On-Demand server through a browser.
9. Run the following command to extract the files:

   ```
   unzip [cd_rom]:\zip\hod60www.zip
   ```

10. If you unpacked `hod60www.zip` into `SYS:\web\docs` as suggested above, the `HOD` directory is automatically published, because it is a subdirectory of the default published directory, `SYS:\web\docs` . If you unpacked the file anywhere else, publish that directory (make it available to client users who access the server through a browser). Refer to the Web server documentation for information about how to do that.
11. Reboot the server.
12. From the server console, run the command `load java` to start the Java NLM.
13. Start the Host On-Demand Service Manager, which provides support services for Host On-Demand and runs as a Java application, by following these steps from a client system mapped to the `SYS` volume of the server:
    a. Change directory to the `\hostondemand\lib` subdirectory.
    b. Copy `NCServiceManager-Novell.ncf` from the `\hostondemand\lib\samples\CommandFiles` directory to the `\system` directory on the Novell Server. To run the command from the server console, you might have to change the filename to the eight-dot-three format.
    c. Edit `NCServiceManager-Novell.ncf` (or the eight-dot-three format of the file) to reflect the directory paths that are correct for your workstation.
    d. From the server, run `NCServiceManager-Novell.ncf` (or the eight-dot-three format of the file). The Service Manager does not display a message indicating that it has started.

For Host On-Demand to function, the Service Manager must be running. If you reboot the server, you must also restart the Service Manager.

14. Restart the Web server.
15. Load `HODMain.html` , located in the `\hostondemand\HOD` directory, into your browser.
    - Click readme to see the latest information.
    - Click Basic configuration steps to help you get started with configuring the Host On-Demand server.

Installing on AIX

To install Host On-Demand on AIX, the following are required:

- AIX Web server
- JVM 1.1.8 or 1.3

You can automatically install Host On-Demand through a graphical interface, or through an ASCII control file in silent mode.

The automatic installation verifies the presence and version of required products before installation occurs. If a prerequisite is missing the action taken by the Install Manager will depend on the policy setting in the control file.

Installing Host On-Demand using the graphical interface

To install the Host On-Demand server on a AIX workstation using the graphical interface, follow the steps below.

1. Insert the CD and mount the CD-ROM drive.

2. Start the installation program by changing to the root directory of the CD, type `setupaix.sh` and press Enter. You may need to type `./setupaix.sh` if the current directory (.) is not set in your `PATH` variable.
3. You may click on View Documentation.

Make sure you have configured Netscape such that it can be run by the installation program. Specifically, before running setupaix.sh, ensure that the Netscape executable is in your PATH (e.g. /usr/local/netscape), and that MOZILLA_HOME is set to the appropriate directory (e.g. /usr/local/netscape).

4. Click Install Product.
5. Follow the directions in the installation windows.
   - The default server directory, determined by the installation program, is `/usr/opt/hostondemand` . The server directory contains files used only by the server and must not be available to client workstations.
   - The default publish directory, determined by the installation program, is `/usr/opt/hostondemand/HOD` . The publish directory contains files that must be available to client users who access the server through a browser.
   - The default Service Manager port is 8999, and it is usually a safe port to select. Check your server documentation to see if this port is being used. If it is in use, you can change the port later. For more information about changing the Service Manager port, see Changing the Service Manger's configuration port in the online help.
6. If you have not already done so, read the `readme` file available in the last window. Click finish to end the installation.
7. If a message tells you that your Web server was not recognized or was not configured, configure it. If you install a Web server later or your Web server was not recognized by the Install Manager, you must publish the Publish directory to the Web. Refer to the Web server documentation for information on how to publish the directory.
8. Restart the Web server.
9. Load `HODMain.html` , located in the `/usr/opt/hostondemand/HOD` directory, into your browser. This page contains links to all the Host On-Demand clients, the readme file, and basic configuration steps for configuring the Host On-Demand server.

Installing Host On-Demand in silent mode

A silent installation installs Host On-Demand without displaying any windows or asking for input. All of the input required during an installation is obtained from a text file called a response file. A response file is created by recording an installation.

When you install in silent mode, there is no indication that installation is in progress or that it is complete.

Options supported in silent mode

Command Line Option	Description
-r	Records a response file.
-p	Runs a response file to install Host On-Demand.

/path/response_file_name	Defines the name for the response file. The default is install.script, and a sample install.script file is provided in the \instmgr directory on the Host On-Demand CD. Any file name can be used if properly specified on the command line used to execute the installation process.

Below are sample command lines that will install Host On-Demand on an AIX workstation in silent mode. The silent mode installation installs Host On-Demand in the `/usr/opt` directory, creates `hostondemand` as the server directory and `HOD` as the publish directory. The examples assume that you mounted the CD-ROM drive as `/cdrom` .

The following commands must be on one line. Before issuing any of the following commands change into the instmgr directory, for example. `cd /cdrom/instmgr`.

To install in silent mode using the `install.script` from the CD and record a log file called HodInstall.log:

```
/cdrom/instmgr/installaix.sh -p /cdrom/instmgr/install.script > /tmp/HodInstall.log
```

To record a response file:

```
/cdrom/instmgr/instaix.sh -r /tmp/install.script
```

To playback the response:

```
/cdrom/instmgr/instaix.sh -p /tmp/install.script
```

The target system's configuration **must** be the same as that of the source system (the system on which the response file was created). For example, if the source system has a previous installation of Host On-Demand Version 6, the target system must have the same. If the source system installed Host On-Demand to a `/usr/opt/hostondemand` directory, the target system must also have a `/usr/opt/hostondemand` directory. The source and target systems must have the same number of Web servers, though they do not need to be the same type.

Installing on UNIX (Solaris, HP-UX, and Linux)

To install Host On-Demand on Solaris, the following are required:

- Solaris Web server
- JVM 1.1 8 or 1.3

To install Host On-Demand on HP-UX, the following are required:

- HP Web server
- JVM 1.1.8 or 1.3

To install Host On-Demand on Linux, the following are required:

- Linux Web Server
- JVM 1.1.8 or 1.3

Host On-Demand Version 6 does not work with the Gnome 1.0 desktop, using the default window manager, Enlightenment. You must upgrade to Gnome 1.2 or later and use the new default window manager, SawFish.

Obtain the latest JDK for UNIX from one of the following sites:

```
http://www.ibm.com/java
ftp://ftp.hursley.ibm.com/pub/java
```

If you have previously installed Host On-Demand and have changed /hostondemand/lib/NSMprop or changed or created /hostondemand/hod/config.properties , you must back up these files before installation, then restore them after installation. The files are overwritten during the installation process.

To install the Host On-Demand server on a UNIX workstation, follow the steps below. These examples assume that you are installing Host On-Demand in the /usr/local directory and that hostondemand is the server directory and HOD is the publish directory. Adjust the statements to match your environment.

1. Insert the CD and mount it.
2. Create a server directory, for example, hostondemand . The server directory contains files that are used only by the server and must not be available to client workstations.
3. Change to the server directory.
4. Tar files are located in the /cdrom/tar directory. Untar the files from hod60srv.tar to the server directory.
5. Untar hod60www.tar into the HOD directory. English language support is installed by default. If you want additional language support, untar the appropriate language file from the /cdrom/tar directory. For example, to install Spanish language support:

   ```
   cd HOD
   tar -xf /cdrom/tar/hod_es.tar
   ```

6. In this example, assume that the tar files are in the /cdrom/tar directory. These commands create the /usr/local/hostondemand and /usr/local/hostondemand/HOD directories and install the files.

   ```
   cd /usr/local
   mkdir hostondemand
   cd hostondemand
   tar -xf /cdrom/tar/hod60srv.tar
   mkdir HOD
   cd HOD
   tar -xf /cdrom/tar/hod60www.tar
   ```

7. Make the publish directory, /usr/local/hostondemand/HOD available to clients on the network. Refer to your Web server documentation for information about how to do that.
8. Start the Host On-Demand Service Manager, which provides support services for Host On-Demand and runs as a Java application:
   a. Change directory to the /usr/local/hostondemand/lib subdirectory.
   b. Copy NCServiceManager-UNIX from the /usr/local/hostondemand/lib/samples/CommandFiles directory.

Make sure the NCServiceManager-UNIX file has execute permission.

   c. Edit NCServiceManager-UNIX to reflect the directory paths that are correct for your workstation.

d. Run `NCServiceManager-UNIX` . The Service Manager does not display a message indicating that it has started. To arrange for this script to be run at boot time, refer to the documentation supplied with your operating system to add a boot service.

For Host On-Demand to function, the Service Manager must be running. If you reboot the server, you must also restart the Service Manager.

9. Restart the Web server.
10. Load `HODMain.html`, located in the `hostondemand/HOD` directory, into a browser.
    - Click readme to see the latest information.
    - Click Basic configuration steps to help you get started with configuring the Host On-Demand server.

Installing on OS/400

The following are required for installing Host On-Demand on an iSeries server:

- TCP/IP Connectivity Utilities for AS/400
- One of the following HTTP servers:
  - IBM HTTP Server for AS/400
  - Lotus Domino for AS/400
  - Apache-based HTTP Server for AS/400
- Java Developer's Kit
- IBM Java Toolbox
- QShell Interpreter
- 256MB memory or more. Refer to the AS/400 Performance Capabilities Reference Web page for additional information about the impact of additional memory and Java performance
- Recent cumulative service is recommended. Refer to the OS/400 Fixes, Downloads and Updates Web page for service information

Installing Host On-Demand

1. Sign on to the iSeries with the `QSECOFR` user profile (or user profile with equivalent security authorities).
2. If Host On-Demand has previously been installed, issue the following OS/400 command to shutdown the Service Manager:

   ```
   ENDHODSVM
   ```

3. If you previously installed Host On-Demand, type the following commands to back up the current settings:

   ```
   CRTSAVF QGPL/HOD

   SAV DEV('/qsys.lib/qgpl.lib/hod.file')
      OBJ(('/qibm/proddata/hostondemand/private/*')
      ('/QIBM/ProdData/hostondemand/lib/NSMprop')
      ('/QIBM/ProdData/hostondemand/hod/config.properties'))
   ```

   Note: The line beginning with `SAV` and ending with `.properties'))` should be one line on your command line.
4. Place the Host On-Demand for OS/400 CD in the iSeries CD drive.
5. Type the following OS/400 command:

   ```
   RSTLICPGM LICPGM(5733A59) DEV(OPT01)
   ```

This command will process for 10-45 minutes, depending upon the configuration of the iSeries.

6. For each additional OS/400 secondary language that you would like to provide full help text support for, type the following OS/400 command:

   ```
   RSTLICPGM LICPGM(5733A59) DEV(OPT01) LNG(xxxx) RSTOBJ(*LNG)
   ```

   Where *xxxx* is the language code from the list below. This step is optional and can be performed after installation.

Language	Language code
Belgian Dutch	2963
Belgian English	2909
Belgian French	2966
Brazilian Portuguese	2980
Canadian French	2981
Chinese (simplified) PRC	2989
Chinese (traditional) Taiwan	2987
Czech	2975
Danish	2926
Dutch Netherlands	2923
English	2924
English DBCS (uppercase)	2938
English (uppercase)	2950
English DBCS	2984
Finnish	2925
French	2928
French Multinational	2940
German	2929
German Multinational	2939
Greek	2957
Hungarian	2976
Italian	2932
Italian Multinational	2942
Japanese Kanji DBCS	2962
Korean DBCS	2986
Norwegian	2933
Polish	2978
Portuguese	2922
Portuguese Multinational	2996
Russian	2979
Slovenian	2911
Spanish	2931
Swedish	2937
Thai	2972

Turkish	2956

7. If you have previously installed IBM Screen Customizer, you must install the new version at this time. Refer to the installation manual for Screen Customizer.
8. If you want the Host On-Demand Service Manager to automatically start after an IPL (when QSYSWRK is started), type the following OS/400 command:

   ```
   CFGHODSVM AUTOSTART(*YES)
   ```

9. To view the status of the Host On-Demand Service Manager, type the following OS/400 command:

   ```
   WRKJOB QHODSVM
   ```

   To restore the former configuration settings (if Host On-Demand was previously installed), type the following command:

   ```
   RST DEV('/qsys.lib/qgpl.lib/hod.file')
       OBJ(('/qibm/proddata/hostondemand/private/*')
       ('/QIBM/ProdData/hostondemand/lib/NSMprop')
       ('/QIBM/ProdData/hostondemand/hod/config.properties'))
       OUTPUT(*PRINT) ALWOBJDIF(*ALL)
   ```

   Note: The line beginning with `RST` and ending with `ALWOBJDIF(*ALL)` should be one line on your command line.

Configuring the OS/400 HTTP server

The following commands assume that you are using the `DEFAULT HTTP` configuration and `CONFIG HTTP` instance. These adjustments are necessary to grant the HTTP server permission to serve objects from the `/qibm/proddata/hostondemand/hod` directory. Refer to the iSeries Webmaster's Guide `http://as400bks.rochester.ibm.com` for additional information.

1. Stop the Web server using the following command:

   ```
   ENDTCPSVR *HTTP HTTPSVR(DEFAULT)
   ```

2. Configure the Web server using the following command:

   ```
   WRKHTTPCFG
   ```

3. Make sure that active `Enable POST` and `Enable GET` entries exist and are not commented out. Add the following entry (there must be one space before the first slash (/) and after the first asterisk (*)):

   ```
   pass /hod/* /QIBM/ProdData/hostondemand/HOD/*
   ```

   This entry creates an alias, `hod` , for the path to the Host On-Demand files. You must type it exactly as you typed the original directory names, matching upper and lower case.

4. Press F3 to exit the `WRKHTTPCFG` tool.
5. Start the Web server using the following command:

   ```
   STRTCPSVR *HTTP HTTPSVR(DEFAULT)
   ```

6. If you want the Host On-Demand Service Manager to automatically start after an IPL (when QSYSWRK is started), type the following command:

   ```
   CHGHTTPA AUTOSTART(*YES)
   ```

7. Load http://*server_name*/*hod_alias*/hodmain.html (where *server_name* is the name of your server and *hod_alias* is the directory you set in step 3 above) to verify that the Web server can serve Host On-Demand HTML pages.

Configuring, starting, and stopping the Host On-Demand Service Manager on iSeries

A menu is provided for starting and stopping the Host On-Demand Service Manager. To access the menu, type the following on the OS/400 command line:

```
GO HOD
```

The following commands can be used from the menu or the OS/400 command line.

Configure (CFGHODSVM): To configure the Service Manager, choose option 1. You need *JOBCTL and *ALLOBJ authority to use this option. You can configure the following information:

1. Whether to autostart the server when the subsystem starts
2. Adjustment of Java attributes
3. The user ID that the server job uses
4. The subsystem that the server job uses
5. The job description that the server job uses
6. The pre-start class/job priority that the server job uses

There are multiple screens. You may need to page down to see the next screen.

Start (STRHODSVM): To start the Host On-Demand Service Manager, choose option 2. You need *JOBCTL authority to use this option.

The Service Manager can be automatically started each time that the associated subsystem starts. One way to do this is to add the STRHODSVM command to the system startup program.

To determine whether the Service Manager is running, use the following command:

```
WRKJOB QHODSVM
```

Stop (ENDHODSVM): To stop the Service Manager, choose option 3. You need *JOBCTL authority to use this option.

Problem determination: If Host On-Demand does not run, it may be that the Service Manager did not start correctly. In this case:

1. Choose option 4 from the menu.
2. Wait a few minutes.
3. Review the list of Java classes that were not loaded.
4. Use the `WRKLNK` command to locate the missing classes.
5. Adjust the Java classpath settings using the `CFGHODSVM` command.
6. Repeat the process until all errors are fixed.

To use the Deployment Wizard to deploy screens to an iSeries-based Host On-Demand server, do the following:

1. Install Host On-Demand on a Windows server platform.
2. On the windows server system, map a network drive to the `\\>iseries.name.com<\qibm` directory. For additional information, refer to `http://publib.boulder.ibm.com/html/as400/v5r1/ic2924/info/rzahl/rzahlusergoal.htm`.
3. Design screens on the Deployment Wizard.

4. Save the customized HTML page to the `y:\ProdData\hostondemand\hod directory`.
5. Using a browser, test out the Web page (for example, `http://iseries.name.com/hod/myweb.html`).

For advanced configuration information, see Configuring on iSeries in Appendix C.

Installing on z/OS

For instructions about installing Host On-Demand on z/OS, refer to the program directory supplied with the z/OS or legacy OS/390 program product.

Installing the configuration servlet

During the Host On-Demand installation, you can choose to have the configuration servlet installed and configured on Windows NT and 2000 for recognized Web application servers. Recognized Web application servers include:

- IBM WebSphere Application Server Version 3.5
- Lotus Domino Go Web Server
- IBM Domino Go Web Server

You can choose to have the configuration servlet installed and configured on AIX if WebSphere Application Server Version 3.5 is detected.

You must manually install the Host On-Demand configuration servlet on operating systems where the servlet is not automatically installed. To manually install the configuration servlet for OS/400, there is a sample shell script in /QIBM/ProdData/hostondemand/lib/samples/HodServlet/CfgHodServlet-OS400.sh.

All Web servers and servlet engines are configured differently. Check your Web server and servlet engine documentation for servlet configuration details on your operating system.

The following instructions assume a Web server is already installed on Windows NT. To manually install the configuration servlet:

- Install Host On-Demand, without running the configuration servlet installation, to a directory such as `d:\hostondemand` .
- Add `cfgsrvlt.jar` from the Host On-Demand installation's `lib` directory to the servlet engine's classpath; for example `d:\hostondemand\lib\cfgsrvlt.jar` . Refer to your Web server or servlet engine documentation for information about how to do this. You can get a copy of `cfgsrvlt.jar` from the `/servlet` directory of the Host On-Demand CD, or from the `/hostondemand/lib` directory where you installed Host On-Demand on your server.
- Add a servlet definition named `hodconfig` with a class name of `com.ibm.eNetwork.HODUtil.services.remote.HODCfgServlet`. Refer to your Web server or servlet engine documentation for information about how to add a servlet definition.
- Configure the configuration servlet. If necessary, set the `ConfigServer` and `ConfigServerPort` parameters to the host name and port number of the Host On-Demand Service Manager. Refer to your Web server or servlet engine documentation for information about how to pass parameters to a servlet.

The port used by the clients, configuration servlet, and the Service Manager can be customized. For instructions on how to customize the port, see configuring the configuration servlet and changing the Service Manager port in the online help.

The Host On-Demand clients use the default port of 8999 to communicate with the Service Manager for configuration information. If any of your clients are outside the firewall, the firewall administrator must open this port internally and externally. Optionally, you can customize the clients to access the configuration servlet through a firewall over either HTTP or HTTPS. The configuration servlet then communicates with the Service Manager on port 8999. If both the configuration servlet and the Service Manager are inside the firewall, port 8999 does not need to be opened for Host On-Demand.

- Publish the `hodconfig` servlet with an alias of `/servlet/hodconfig`. Refer to your Web server or servlet engine documentation for information on about how to make the configuration servlet known to the Web server. In general, you are associating the fully qualified name of the servlet with an alias, such as `/servlet/hodconfig/hod`.
- Stop and restart the Web server and the servlet engine, or refer to your Web server or servlet engine documentation for information about saving the changes.

Once the configuration servlet is installed, you must configure your clients to use the configuration servlet instead of directly accessing the Service Manager. You can use the Deployment Wizard to build customized HTML client pages. The wizard sets the applet parameters in the HTML based on your input, so you don't have to learn the syntax and valid parameter values. We recommend that you use the Deployment Wizard to set the ConfigServerURL parameter in the client HTML to the name you assigned to the servlet through the servlet engine in the publish step above. For example, if you set the name of the servlet to be `/servlet/hodconfig`, set the Configuration Server URL to `/servlet/hodconfig/hod`.

The servlet alias and the value for the `ConfigServerURL` parameter are different.

If you find you need to manually modify the HTML, use the *<param tag>* inside the *<applet>* tag to set the ConfigServerURL. For example, to set the `ConfigServerURL` to `/servlet/hodconfig/hod` set `<param name=ConfigServerURL value=/servlet/hodconfig/hod>` in the *<applet>* tag in the HTML client.

For more information regarding configuration servlet parameters, configuration and examples, see Configuring the configuration servlet in the online help.

Chapter 4. Migrating from previous versions of Host On-Demand

With very few exceptions, data used in earlier versions of Host On-Demand will be automatically migrated when you begin using Host On-Demand Version 6.

Any existing configuration data in your configuration server will be automatically available in Host On-Demand Version 6 once installation is complete.

Existing custom HTML files must be edited and saved with the Deployment Wizard in order to take advantage of new Host On-Demand Version 6 features. Users who access these updated HTML files will automatically begin benefitting from the new Host On-Demand Version 6 functions; and any local configuration data will be seamlessly migrated for them.

Custom HTML files which are not updated with the Deployment Wizard will generally still work, but they will not have any new Host On-Demand Version 6 functionality. If you are using Screen Customizer in these older HTML files, and you do not want to edit them with the Deployment Wizard, you will need to manually edit the HTML files to change all existing occurrences of scbase.jar and scbase.cab to sccbase.jar and sccbase.cab, respectively.

Existing cached client HTML files will not work with Netscape 6.x or other browsers running with JRE 1.3. You must update these files using the Deployment Wizard. Existing Download client HTML files will work with Netscape 6.x if:

1. The files were customized using a previous version of the Deployment Wizard.
2. The client does not attempt to use any new function that was not included from the Preload Options page when the HTML file was created by the Deployment Wizard.

Chapter 5. Removing Host On-Demand

To remove the Host On-Demand server:

Windows NT or 2000
Use Add/Remove Programs from the Windows control panel.

UNIX Stop the Host On-Demand Service Manager. Get the process ID, kill the process, then delete the Host On-Demand directories (except `./private`).

OS/2 Stop the Host On-Demand Service Manager by pressing `Ctrl+C` in the OS/2 window in which you started it, close the window, then delete the Host On-Demand directories (except `\private`).

NetWare
From the console, enter `java -exit` to stop the Java NLM, then delete the Host On-Demand directories (except `\private`).

iSeries
You will need `*JOBCTL, *SPLCTL, *SERVICE` and `*ALLOBJ` authority to use this command. Logon to the iSeries with a security officer user profile, such as `QSECOFR` .

1. Shutdown the Service Manager by typing `ENDHODSVM` at the command line.
2. Delete the licensed Host On-Demand product by typing `DLTLICPGM LICPGM(5733A59)` at the command line.
3. Remove any directories containing user data manually after the program has completed. You will also need to remove the `QUSRSYS/QHODCFGD *DTAARA` object.

To remove the cached client:

Load `http://` *server_name*`/`*hod_alias*`/HODRemove.html` in your browser. After displaying a confirmation message, it removes all previous versions of the cached client from all levels of Netscape and Internet Explorer.

With Netscape 6.0 and other Java2-enabled Web browsers, HODRemove will instruct the user to use the Java Control Panel to clear the JRE cache. For more information, see Netscape 6.0 and Java2-enabled Web browser issues.

Chapter 6. Using Host On-Demand with a firewall

If you are configuring Host On-Demand to go through a firewall, make sure the firewall administrator opens port 8999 internally and externally. The Service Manager listens to port 8999 by default, and the client receives configuration information directly from the Service Manager over port 8999 by default. You can customize the port the clients and Service Manager use. To customize the port, see changing the Service Manager port in the Host On-Demand online help.

In addition to port 8999, make sure the firewall administrator opens any ports that are being used for functions your clients use. For example, if you have an SSL session with the Redirector on port 5000, port 5000 must be opened for Telnet traffic. The following table summarizes the ports that Host On-Demand can use.

Host On-Demand Function	Ports Used
Display emulation (5250 and 3270)	23 (Telnet), 80 (HTTP) and 8999 (config server)[3]
Printer emulation (5250 and 3270)	23 (Telnet), 80 (HTTP) and 8999 (config server)[3]
3270 file transfer	23 (Telnet), 80 (HTTP) and 8999 (config server)[3]
5250 file transfer - savfile	80 (HTTP), 8999 (config server)[3], 21 (ftp)[4], >1024 (ftp)[4], 446 (drda)[4], 449 (as-svrmap)[4], 8470 (as-central)[1 2 4], 8473 (as-file)[1 4], 8475 (as-rmtcmd)[1 4], and 8476 (as-signon)[1 4]
5250 file transfer - database	80 (HTTP), 8999 (config server)[3], 446 (drda)[4], 449 (as-svrmap)[4], 8470 (as-central)[1 2 4], 8473 (as-file)[1 4], 8475 (as-rmtcmd)[1 4], and 8476 (as-signon)[1 4]
5250 file transfer - stream file	80 (HTTP), 8999 (config server)[1 2 4], 449 (as-svrmap)[4], 8470 (as-central)[1 2 4], 8473 (as-file)[1 4], and 8476 (as-signon)[1 4]
HODAdmin.html	80 (HTTP) and 8999 (config server)[3]
Database On-Demand	80 (HTTP), 8999 (config server)[3], 449 (as-svrmap)[4], 8470 (as-central)[1 2 4], 8471 (as-database)[1 4], and 8476 (as-signon)[1 4]
License Use Management (LUM)	80 (HTTP)
Deployment Wizard-generated HTML files	23 (Telnet), 80 (HTTP), and 8999 (config server)[3]

Notes:

1 You can change the port numbers with the command `WRKSRVTBLE` . The port numbers listed are the default values.

2 The port for as-central is used only if a code-page conversion table needs to be created dynamically (EBCDIC to/from Unicode). This is dependant on the JVM and the locale of the client.

3 You can change the config server port. Port 8999 is the default.

4 These ports do not need to be opened on the firewall if you are using iSeries proxy server support. You will need to open the default proxy server port 3470. You can change this port.

If you do not want to open port 8999 on the firewall, you can still allow users to access Host On-Demand. There are two options:

- If you want to use the configuration server, you can configure clients to use the configuration servlet. See Configuring the configuration servlet in the Host On-Demand online help. This option is only available if your Web server supports servlets.
- Use the Deployment Wizard to create HTML files that contain all configuration information. This eliminates the need to access the configuration server. When creating the HTML files, choose “HTML-based model” from the Configuration Model page of the Deployment Wizard.

Chapter 7. Configuring Host On-Demand overview

After installing Host On-Demand, you'll need to configure Host On-Demand sessions for your users. To do this, you can use the Deployment Wizard to create HTML files or use the default configuration files shipped with Host On-Demand.

The Host On-Demand Deployment Wizard guides you through the necessary steps to create an HTML page that can be used to launch Host On-Demand host sessions. Using the Deployment Wizard, you can choose from three different configuration models to specify how session configuration information and users preferences (e.g., changes users make to session size and location, colors, etc.) are defined and managed:

- HTML-based model
- Configuration server-based model
- Combined model

If you choose the HTML-based model, all session information is contained in the HTML file itself, and nothing more is needed to define host sessions. After the HTML file is downloaded by clients initially, the session configuration information and user preferences are stored locally on the user's machine.

If you are using the configuration server-based model or the combined model, you must define the sessions in the configuration server. (It may be useful to configure the sessions on the configuration server before creating the HTML file with the Deployment wizard). The configuration server is a part of Host On-Demand that centrally stores session configuration information and user preferences by user and group IDs. Users then access session information and user preferences by contacting the configuration server. The configuration server is managed through the Administration Utility.

In addition to defining how sessions and user preferences are defined and managed, with the Deployment Wizard, you can configure a number of client-side options, such as:

- Whether the Host On-Demand files should be cached for quicker startup
- What components should be included in the initial download (thus determining the size of the initial download)
- What session functions are available to users
- Whether to automatically log users on to Host On-Demand
- Run-time options, such as session size and placement, colors, toolbar customization, and macros
- Display options
- Locale options (for example, what language to display in)

Host On-Demand includes a number of pre-defined HTML files that can be used by users to access sessions. They all use the configuration server-based model, and therefore all require you to define sessions on the configuration server.

Read the Basic Configuration Steps for more detailed information on using the Deployment Wizard and configuring the Host On-Demand configuration server.

Chapter 8. Loading the Host On-Demand clients

The Host On-Demand clients are implemented as HTML files that you load into a Web browser.

There are many ways users can load the clients:

- Customize your own HTML pages to launch sessions that you have configured. You can use the Deployment Wizard to create customized pages. See Deployment Wizard in the Host On-Demand online help for more information.
- Load the `HODMain.html` file, located in the `/hostondemand/HOD` directory, into your browser to view links to all the available clients. You can edit the HTML file and customize its contents to suit your users and their environment. Users won't need to remember the name of the client or the name of the file that is used to load it.
- Load the full URL.

  `http://server_name/hod_alias/client_name.html`

  where *server_name* is the host name or IP address of the Host On-Demand server, *hod_alias* is the alias (or path) of the published directory, and *client_name* is the HTML file name of the client. For example:

  `http://name.city.yourcompany.com/hod/HOD.html`

  will load the default Host On-Demand Download client.

Let users know about the security warning that appears when using Host On-Demand. The purpose of the window is to tell users that Host On-Demand was created by **International Business Machines** and to ask whether they trust it.

Host On-Demand clients

Note: The following table lists the Host On-Demand default clients. These clients use the Configuration server-based model.

Package	Client	HTML File
Administration Clients	Administration client	HODAdmin.html
	Administration client cached	HODAdminCached.html
	Administration client cached with problem determination	HODAdminCachedDebug.html
Emulator Clients	Cached client	HODCached.html
	Cached client with problem determination	HODCachedDebug.html
	Download client	HOD.html
	Download client with problem determination	HODDebug.html
	Download client with Screen Customizer/LE Interface	HODCustom.html
	Function On-Demand client	HODThin.html
Database Clients	Database On-Demand client	HODDatabase.html

Package	Client	HTML File
	Database On-Demand client cached	HODDatabaseCached.html
	Database On-Demand client cached with problem determination	HODDatabaseCachedDebug.html
Utilities	Remove cached client	HODRemove.html
	New user client	NewUser.html
	New user client cached	NewUserCached.html
	New user client cached with problem determination	NewUserCachedDebug.html

Note: Custom-built clients are created by the Deployment Wizard. These will have unique HTML file names.

Administration clients

The Administration client (`HODAdmin.html`) starts the Administration window where you can:

- Manage users, groups, and sessions
- Configure, manage and trace the Redirector service
- Configure Database On-Demand
- Enable security
- View trace and message logs
- Disable functions to end users

You must add users and configure sessions for them before they can access the clients.

Administration client cached (`HODAdminCached.html`)

This client starts the Administration client in a cached environment. Load this HTML page if you want to use the Administration client in cached environment without problem determination. The advantage of the Administration client cached is that it can be cached along with the cached client in the browser. In releases prior to Version 5, the cached client had to be removed before the Administration client could be loaded.

If you want to bookmark the Administrator client cached, you must manually create the bookmark. It must point to HODAdminCached.html, so that Host On-Demand can compare the cached version to the server version. This allows Host On-Demand to recognize and notify you that a newer version of the Administration client cached is available at the server.

Administration client cached with problem determination (`HODAdminCachedDebug.html`)

This client also starts the Administration client in a cached environment. Load this HTML page if you want to use the Administration client in cached environment with problem determination (session logging and tracing).

Cached clients

A cached client can be any client where you choose to cache the applet on the user's machine. Most likely, the HTML is created using the Deployment Wizard; however, it could be HODCached.html, as well. The cached client (`HODCached.html`) provides all the Host On-Demand functions including problem determination and the Screen Customizer. It is cached on your local disk the first time you download it. The next time you start the emulator session, only a small applet downloads from the server, reducing the time needed to start the session. The applet that is downloaded checks to see if the software on the server is more recent than the software that has been cached. If so, the cached software is updated. The cached client is recommended for users with slow connectivity (such as dial-up phone lines) where downloading a large applet would take a long time.

Note: Using the cached client with Netscape 6.x or another Java2-enabled Web browser causes the hoddbg.jar file to be downloaded. This gives the client full Host On-Demand functionality; however, the resulting download will be approximately 4.5MB. It is recommended that you use the Deployment Wizard to customize your HTML files to include only those components that are needed.

The cached client is persistent across operating system restarts and browser reloads. If you want to remove it, you must load http://*server_name*/*hod_alias*/HODRemove.html in your browser, where *server_name* is the name of your Web server and *hod_alias* is the alias you selected during installation.

For more information on removing the cached client from a JRE 1.3 client, see Netscape 6.0 and Java2-enabled Web browser issues.

In order for you as a client-side user on Windows 2000 Professional to successfully install the Host On-Demand cached client, you must have sufficient permissions set to change the system registry. A Windows 2000 "Restricted User (Users group)" user cannot successfully complete a Host On-Demand cached client installation unless granted "Standard User (Power Users group)" access.

Cached client support across the Internet

If you deploy the cached client to the Internet, consider that your users might use Host On-Demand with other business partners running Host On-Demand servers at different service levels. This could be a problem if your user needs different functions when accessing servers at different service levels. Components of different service levels are not supported within a single cached client, and there can be only one cached client on a machine. Host On-Demand Version 5.0.4 or higher is required to run the cached client across the Internet.

To prevent complications, you can do some or all of the following:

- Select all the functions a user needs (across all sites the user accesses) in a preload list when you create an HTML page using the Deployment Wizard
- Use the disable function of the Deployment Wizard to disable all functions not in the preload list and the functions that are not needed for your users
- Create separate HTML pages for different user groups
- Give your HTML pages a name that identifies your company
- Always install Screen Customizer to prevent users who are accessing your server from losing Screen Customizer functions when accessing other sites

If the software on the server is an earlier version than the cached software, the cached client applet checks the version levels of the components and prevents caching of any new components. To cache new components, remove the more recent version of the cached client and then install the earlier version of the cached client. To avoid this problem, select all the functions the user needs (across all sites the user accesses) in the preload list when you create the HTML page using the Deployment Wizard.

When a client points to a server running a later version of Host On-Demand, *and the upgrade test passes, all* cached components are automatically upgraded (not only the components defined in the HTML page's preload list). Because all cached and new components are upgraded at simultaneously, the upgrade might generate additional Web Server load. After the upgrade, the client can point back to the server running the earlier version of Host On-Demand, and the more recent cached client functions correctly.

If you use the cached client on the Internet, you must install Screen Customizer on your server. If a full function version of Screen Customizer is cached and Screen Customizer is not installed on the server, the cached client applet issues an error message and prevents the upgrade.

If you are using locally stored preferences, the custom HTML pages you create must have names unique to your company, because the HTML file names differentiate between the locally stored preferences of different sites. Using generic names could cause preference conflicts for your users.

If you have problems managing cached client deployment on the Internet, see the Host On-Demand support Web site for more information.

Installing the cached client

There are a number of ways to install the cached client. You can install it from the server, or from a local source, such as a CD or a network drive, or you can create an HTML file that specifies the client is a cached client, using the Deployment Wizard.

To install the cached client from the server, you can either:

- Load http://*server_name*/*hod_alias*/HODCached.html (or whatever the name of the file is that you created with the Deployment Wizard)
- Click on the cached client link after loading http://*server_name*/*hod_alias*/HODMain.html (if you want to use this predefined file).

The client begins installing immediately. A new browser window shows the status of the installation. The top progress bar shows the status of individual files as they download. The bottom progress bar shows the status of the overall installation. When the installation is complete, you are prompted to restart the browser.

Note: If you are installing the cached client on Netscape 6.0, or later, or Mozilla, a separate installation progress window will not appear. Also, with these browsers, you do not need to restart the browser before using Host On-Demand.

With Web browsers that use a Java2 Runtime Environment, the HOD jar files are stored in the JRE cache.

To install the cached client from a local source:

Note: If you are installing the cached client on a Netscape 6.0 Web browser, you cannot install the client from CD.

1. Copy the following files from the *HOD* publish directory of your Host On-Demand server installation, to a network drive or put them on a CD:

   ```
   HODCached.html (customized for a LAN or CD load)
   hodlogo.gif
   hodbkgnd.gif
   Installer.html
   Cached.js
   ccversions.properties
   CachedAppletInstaller.*
   CachedAppletSupporter.*
   CachedAppletRemover.*
   sccbase.*
   *.jar
   *.cab
   scccversions.properties
   ```

   These next files are in subdirectories of the *HOD* publish directory of your Host On-Demand server installation. You must keep these files in the appropriate subdirectories when copying them to your LAN or CD drive.

   ```
   msgs\cached_*.properties
   com\ibm\eNetwork\msgs\cached_*.class
   ```

2. Start the browser and open the file `HODCached.html` from the source (CD or directory). The installation begins immediately. You will see a progress bar as the client is installed, then a message asking you to restart the browser. Do so, then enter the URL for the cached client on your Host On-Demand server, not on the local source:

   `http://`*`server_name`*`/hod/HODCached.html`

   From now on, load `HODCached.html` from the server.

If you want to install the cached client using a customized HTML file, you must first create the HTML using the Deployment Wizard. Then load the HTML file from either the server or from a network drive. See the online documentation for the Deployment Wizard for more information regarding creating an HTML file.

Upgrading Host On-Demand Version 4.x cached clients to Host On-Demand Version 6

If you upgrade your Host On-Demand server from Version 4.x to Version 6, your clients will no longer be able to communicate with the server without upgrading.

If you need to manage network demand while upgrading cached clients, you can gradually move all of your Host On-Demand Version 4.x cached clients to Host On-Demand Version 6 by setting up two servers. One would be a Host On-Demand Version 4.x server and the other would be a Host On-Demand Version 6 server. Configure all clients to access the Host On-Demand Version 6 server, and then add the HTML parameter HODServer to HODCached.html, or any of your customized cached client HTML files that are on the Host On-Demand Version 6 server. There are two applets specified in the HTML files. Add the HODServer parameter to the second applet. You can do all of this using the Deployment Wizard; however, if you want to manually modify the applet, the format for the parameter is:

```
<PARAM NAME=HODServer VALUE=http://yourhostname/alias/HODCached.html>
```

where *yourhostname* and *alias* are your Host On-Demand Version 4.x server's hostname and alias, or Publish, directory. The *HODServer* parameter works with the UpgradePercent and UpgradeURL parameters to manage client upgrades. If the cached client won't be upgraded on this connection attempt, it is redirected automatically to the Host On-Demand Version 4.x server specified in the *HODServer* HTML parameter. If a cached client will be upgraded, the Host On-Demand Version 4.x cached client is removed and the Host On-Demand Version 6 cached client is installed. Once the client is upgraded to Host On-Demand Version 6, the HTML parameter is ignored and the client is no longer redirected to the Host On-Demand Version 4.x server. After you have gradually upgraded all your cached clients, you no longer need the Host On-Demand Version 4.x server.

Notes:

- Cached clients are upgraded in the foreground. The upgrade in background option is ignored.
- If you have customized Host On-Demand Version 4.x `HODCached.html` and have called it something different, like `OurHTML.html`, you can:
  - Copy the Host On-Demand Version 6 version of `HODCached.html` to the file `OurHTML.html`;
  - Then add the `HODServer` parameter to `OurHTML.html`. The `HODServer` parameter should specify `http://yourhostname/alias/OurHTML.html` as the Host On-Demand Version 4.x server.
- You can copy the new `HODCached.html`, that includes the `HODServer` parameter, to `AutoHODCached.html` and `AutoHODLaunch.html`, in case these pages are bookmarked by the clients. The `HODServer` parameter in `AutoHODCached.html` should specify the `AutoHODCached.html` page on the Host On-Demand Version 4.x server. The `HODServer` parameter in `AutoHODLaunch.html` should specify the `AutoHODLaunch.html` page on the Host On-Demand Version 4.x server
- If you are using language specific HTML pages (such as `HODCached_es.html`, `AutoHODCached_es.html`, `AutoHODLaunch_es.html`, etc.) you can also add the `HODServer` to these pages.

Troubleshooting

If you find that you cannot load the cached client, check the items described below.

Netscape 4.x:

1. In the browser window, click Edit > Preferences > Advanced.
2. Check Enable Java.
3. Check Enable JavaScript.

Microsoft Internet Explorer 4.0.1:

1. In the browser window, click View > Internet Options > Security.
2. Make sure that the Internet and Local Intranet zones are set to Medium security.

Microsoft Internet Explorer 5.5: After upgrading your browser from Microsoft Internet Explorer 4 to Microsoft Internet Explorer 5.5, you may receive security exceptions in the Java console. When you install the Cached Client, several files are stored into the browser's directory structure. When you upgrade Internet Explorer from Version 4 to Version 5, the browser will no longer know about the CAB files which contain the Host On-Demand cached code. Since the browser cannot find the CAB files, it tries to use the class files directly from the server, causing security

exceptions. To resolve this, following a version upgrade of your browser, you should remove Host On-Demand using HODRemove.html, and then re-install the product using HODCached.html.

Cached client with problem determination (HODCachedDebug.html)

This client starts the cached client with problem determination (session logging and tracing).

Loading the download client after installing the cached client

If you have installed the cached client and then wish to load any of the download clients, such as HODAdmin.html or HODDatabase.html, you must first remove the cached client from the browser by loading HODRemove.html in your browser, and then restart your browser. If you do not remove the cached client before loading the Download client the session will not start, and you may see exceptions in the Java console.

Download clients

The Download client (`HOD.html`) provides all Host On-Demand client function, except problem determination. Unlike the cached client, the Download client is downloaded from the server every time you want to use it.

Accessing HOD.html with a browser using the 1.3 JRE (such as Netscape 6.0) will work with limited functions. A list of functions that will not work is contained in Limitations. Using HODDebug.html instead will result in full functionality for Host On-Demand. However, the hoddbg.jar file that is downloaded will be approximately 4.5 MB. It is recommend that you use the Deployment Wizard to customize your HTML files to include only those components that are needed.

Use this client if:

- You do not want to take up disk space on client machines by installing the cached client or the Locally-installed client
- You cannot use the cached client because you don't have a suitable browser.
- Your initial download time is not an issue.

Download client with Screen Customizer/LE Interface (HODCustom.html)

This is the standard client with a window-like interface provided by Screen Customizer. It is downloaded from the server each time it is used.

Download client with problem determination (HODDebug.html)

This client loads the standard Download client with problem determination (session logging and tracing).

Function On-Demand client

Note: This is not available for the Java2-enabled Web browsers, such as Netscape 6.0.

It is recommended that you use the Deployment Wizard to create a customized HTML file instead of the Function On-Demand client.

The Function On-Demand (`HODThin.html`) client is much smaller than the other clients. Initially, only the basic functions are downloaded, so the startup time is greatly reduced. Other functions are downloaded when they are needed. Some

functions might be required immediately (such as the 3270 emulator), while other functions (file transfer, for example) might never be invoked or might not be needed for a long time.

The Function On-Demand client can be configured with the traditional ″green screen″ interface, or it can be configured with the Screen Customizer/LE interface.

You can also create your own Function On-Demand client using the Deployment Wizard, specifying what functions are enabled and what functions download initially.

The Function On-Demand client is downloaded from the server every time you want to use it.

Database On-Demand clients

The Database On-Demand client (`HODDatabase.html`) provides users with a means of making Structured Query Language (SQL) requests to iSeries databases through a Java database connectivity (JDBC) driver. Users can save the results of their requests and use them in other applications, such as a spreadsheet.

Database On-Demand client cached (HODDatabaseCached.html)

This client starts the Database On-Demand client in a cached environment. Load this HTML page if you want to use the Database On-Demand client in a cached environment without problem determination. The advantage of the Database On-Demand cached client is that it can be cached along with the Host On-Demand cached client in the browser.

Note: If your client is going to use multiple code pages, you need to add the appropriate archive (.jar/.cab) file of each code page to the preload list of your cached HTML. For a list of code-page languages and corresponding .jar file names, see Database On-Demand overview.

Database On-Demand client cached with problem determination (HODDatabaseCachedDebug.html)

This client also starts the Database On-Demand client in a cached environment with problem determination. Load this HTML page if you want to use the Database On-Demand client in cached environment with problem determination (session logging and tracing).

Remove cached client

The remove cached client (`HODRemove.html`) removes all previous versions of the cached client from all levels of Netscape and Internet Explorer.

Load `http://` *server_name*`/`*hod_alias*`/HODRemove.html` in your browser. After displaying a confirmation message, it removes all previous versions of the cached client from all levels of Netscape and Internet Explorer. With Netscape 6.0 and other Java2-enabled Web browsers, HODRemove will instruct the user to use the Java Control Panel to remove the JRE cache.

For more information, see Netscape 6.0 and Java2-enabled Web browser issues.

New user clients

Users can use the New User client (`NewUser.html`) to create new accounts, if you check Allow users to create accounts in the Users/Groups window.

New user client cached (NewUserCached.html)

This client starts the New User client in a cached environment. Load this HTML page if you want to use the New User client in a cached environment without problem determination.

New user client with problem determination (NewUserCachedDebug.html)

This client starts the New User client in a cached environment with problem determination. Load this HTML page if you want to use the New User client in a cached environment with problem determination (session logging and tracing).

Chapter 9. Security

Whether you are implementing Host On-Demand purely within your corporate network, or you are using it to provide access to your host systems over the Internet, security is a concern. Host On-Demand uses Secure Sockets Layer (SSL) protocol to provide security for emulator sessions. SSL is an industry-standard protocol that provides encryption and authentication on connections across a TCP/IP network, using X.509 certificates. Host On-Demand supports encryption of emulation sessions and server/client authentication according to the SSL Version 3 standard.

Support is provided for the following:

- RSA type-4 data encryption on connections between the Host On-Demand emulators and Telnet servers that support SSL Version 3
- X.509 certificates
- Bulk encryption algorithms using keys up to 168 bits in length
- Authentication algorithms using keys up to 1024 bits in length
- Server and client authentication
- Support for storage and use of client certificates on the client system
- Optional prompting of user for client certificate when requested by server

A Certificate Wizard (Windows NT, Windows 95, Windows 98 and Windows 2000 only) and a graphical Certificate Management utility are provided to:

- Create certificate requests
- Receive and store certificates
- Create self-signed certificates

Using SSL

SSL is supported only on Windows NT and AIX redirectors, and on clients that have Netscape Communicator 4 or Microsoft Internet Explorer 4 or later browsers.

Host On-Demand provides secure connections between the following:

- A client and the Host On-Demand Redirector or other Telnet server that supports SSL
- Two Host On-Demand redirectors

There are several security options that you can configure. Configuring all of them provides the most security possible:

TLS-based Telnet Security
: You can allow the security negotiations between the client and the Telnet server to occur on the established Telnet connection for Host On-Demand 3270 display and printer sessions, if the Telnet server supports this option. See Telnet-negotiated security in the Host On-Demand online help for more information.

Server authentication
: Encrypting the data exchange between the client and the server does not guarantee the client is communicating with the correct server. To help avoid this danger, you can enable server authentication, so that the client,

after making sure that the server's certificate can be trusted, checks whether the Internet name in the certificate matches the Internet name of the server. If they match, the SSL negotiation will continue. If not, the connection ends immediately. See server authentication in the Host On-Demand online help for more information.

Client authentication
Client authentication is similar to server authentication except that the Telnet server requests a certificate from the client to verify that the client is who it claims to be. Not all servers support client authentication, including the Host On-Demand Redirector. To configure client authentication, you must: obtain certificates for clients; send the certificates to the clients; and configure the clients to use client authentication. See configuring clients to use client authentication in the Host On-Demand online help for more information.

Express logon
You can provide users with an easy host logon process by allowing a user to log on without having to enter a user ID and password. Using this function reduces the time spent by an administrator maintaining host user IDs and passwords. To use Express Logon, the session must be configured for SSL and client authentication. See Express logon in the Host On-Demand online help for more information.

To use server or client authentication, you must first enable SSL.

How SSL security works

SSL uses public-key and symmetric-key cryptographic technology. Public-key cryptography uses a pair of keys: a public key and a private key. Information encrypted with one key can be decrypted only with the other key. For example, information encrypted with the public key can be decrypted only with the private key. Each server's public key is published, and the private key is kept secret. To send a secure message to the server, the client encrypts the message by using the server's public key. When the server receives the message, it decrypts the message with its private key.

Symmetric-key cryptography uses the same key to encrypt and decrypt messages. The client randomly generates a symmetric key to be used for encrypting all session data. The key is then encrypted with the server's public key and sent to the server.

SSL provides three basic security services:

Message privacy
Achieved through a combination of public-key and symmetric-key encryption. All traffic between an SSL client and an SSL server is encrypted using a key and an encryption algorithm negotiated during session setup.

Message integrity
Ensures that SSL session traffic does not change en route to its final destination. SSL uses a combination of public/private keys and hash functions to ensure message integrity.

Mutual authentication

Exchange of identification through public-key certificates. The client and server identities are encoded in public-key certificates, which contain the following components:

- Subject's distinguished name
- Issuer's distinguished name
- Subject's public key
- Issuer's signature
- Validity period
- Serial number

You can also use secure HTTP (HTTPS) to ensure that a client's security information is not compromised as it is downloaded from a server.

An SSL session is established in the following sequence:

1. The client and the server exchange hello messages to negotiate the encryption algorithm and hashing function (for message integrity) to be used for the SSL session.
2. The client requests an X.509 certificate from the server to prove its identity. Optionally, the server can request a certificate from the client. Certificates are verified by checking the certificate format and the validity dates and by verifying that the certificate includes the signature of a trusted certificate authority (or is self-signed).
3. The client randomly generates a set of keys that is used for encryption. The keys are encrypted with the server's public key and securely communicated to the server.

Certificates, encryption, and authentication

Security is controlled by certificates that act as electronic ID cards. These are usually issued by Certificate Authorities (CAs), which are organizations that are trusted by the industry as a whole and whose business is the issuing of Internet certificates. A CA's certificate, which is also known as a root certificate, includes (among other things) the CA's signature and a validity period. For Host On-Demand, you can use a CA's certificate, but you can also create and sign your own. The purpose of a certificate is to assure a program or a user that it is safe to allow the proposed connection and, if encryption is involved, to provide the necessary encryption/decryption keys.

Encryption and authentication are performed by means of a pair of keys, one public, one private. The public key is embedded into a certificate, known as a site or server certificate. The certificate contains several items of information, including the name of the Certificate Authority (CA) that issued the certificate, the name and public key of the server or client, the CA's signature, and the date and serial number of the certificate. The private key is created when you create a self-signed certificate or a CA certificate request and is used to decrypt messages from clients.

To support SSL services, Host On-Demand uses two databases:

HODServerKeyDb.kdb

Is created the first time you configure SSL for the Host On-Demand Redirector. This database contains the server's private key and certificate, and a list of CAs. Because the CAs are included in the file, they are called

well-known or *trusted* to the Redirector. You can add certificates from other CAs (unknown CAs) and certificates that you create and sign yourself (self-signed) to this database.

CustomizedCAs.class
Is created and updated during SSL configuration. This database contains server and CA-root certificates that are not in the well-known list and are needed by Host On-Demand clients.

Examples of when to use SSL security

Some situations where you might want to use SSL security include:

- You want to let customers order your products over the Internet. You want to make sure information they give you, such as a credit-card number, is encrypted so that it cannot be stolen. You also want to make sure information you give to customers is protected.
- You want to give your suppliers or business partners access to certain information on your host computers and to be sure that the data is not available to anyone else.
- You want your staff to have access to your host-computer information from remote sites or when they are traveling.
- You are a hospital administrator and want doctors to have access to patient records from wherever they are and to be sure that the records cannot be seen by unauthorized people.

Using the Redirector

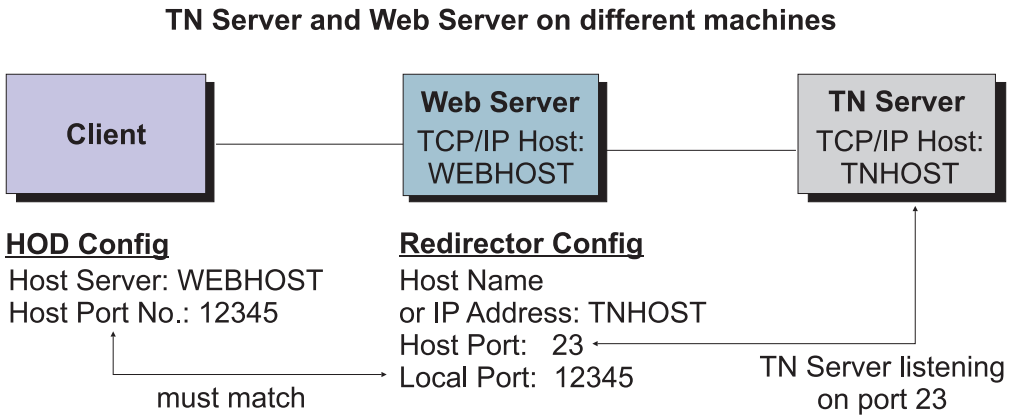
On Windows NT and AIX, the Redirector provides support for Secure Sockets Layer (SSL) security between clients and the Host On-Demand server.

The Redirector acts as a transparent Telnet proxy that uses port remapping to connect the Host On-Demand Server to other Telnet servers. Each defined server can configure a set of local-port numbers. Instead of connecting directly to the target Telnet server, a client connects to the Host On-Demand server and port number. The Redirector maps the local-port number to the host-port number of the target and makes a connection.

Redirectors can be connected to each other (in a cascaded configuration). In that case, SSL security is also available between the redirectors (Windows NT and AIX only).

How the Redirector works

The following scenario shows how the Redirector works. Secure connections are possible between the client and Host On-Demand server.



The Redirector sets security for each local port. Security choices are:

- Pass-through - data between the client and the host is not altered
- Client side - encrypts data between the client and the redirector
- Host side - encrypts data between the redirector and the host
- Both - encrypts data both ways

You must enable security for the Redirector before you can enable client-side security, server-side security or both.

You can use pass-through when encryption by the Redirector is not necessary, either because the data-stream does not need to be encrypted, or because the data-stream is already encrypted between the client and the host. You must use pass-through if the Host On-Demand client is connecting through the Redirector to a host that requires client authentication.

Telnet-negotiated security

Telnet-negotiated security allows the security negotiations between the client and the Telnet server to be done on the established Telnet connection. You can configure Telnet-negotiated security for Host On-Demand 3270 display and printer sessions. It is based on INTERNET-DRAFT TLS-based Telnet Security, which defines extensions to Telnet so that Transport Layer Security (TLS) can be negotiated over a Telnet connection. The TLS Protocol 1.0 allows security negotiation down from TLS 1.0 to SSL. Host On-Demand clients will always negotiate down to SSL Version 3, since Host On-Demand supports INTERNET-DRAFT TLS-based Telnet security, but not TLS Protocol 1.0.

The Telnet server must support TLS-based Telnet security for the Host On-Demand clients to use Telnet-negotiated security. The Communications Server for OS/390 Version 2 Release 10 and later supports TLS-based Telnet security. Communications Server for OS/390 documentation refers to Telnet-negotiated security as ″negotiable SSL.″

For more information regarding Telnet-negotiated security, see Telnet-negotiated security overview in the Host On-Demand online help.

For assistance in configuring Telnet-negotiated security on a 3270 display or printer session, see configuring Telnet-negotiated security; in the Host On-Demand online help.

Chapter 10. LDAP support

A Lightweight Directory Access Protocol (LDAP) server directory provides the ability to share user and group configuration information.

The following LDAP servers are supported for use with Host On-Demand:

IBM LDAP Directory Server V2.1, V3.1.1, and V3.2.1	Windows NT and AIX
Netscape Directory Server V3.1 and V4.0	Windows NT and AIX
IBM LDAP Directory Server running on OS/390 Version 2, Release 5, 6, 7, 8, 9, 10, 11, and 12	Legacy OS/390 and z/OS

Installing LDAP support

1. Decide which LDAP Directory server you are going to use and if necessary install it. For more information on IBM's LDAP Directory solution and to download a complimentary evaluation kit, go to `http://www.software.ibm.com/network/directory/`.
2. Install the Host On-Demand schema extension files. (The schema extension files are not required for IBM LDAP Version 3.x.)
3. Ask your LDAP administrator for a suffix which Host On-Demand will use to store configuration information. Make a note of the distinguished name (DN) of this suffix; you will need this information to complete the LDAP setup.
4. Ask your LDAP administrator for an administrator DN and password for Host On-Demand; these will be used to authenticate to the LDAP server. The administrator DN must have create, modify and delete privileges for the suffix mentioned in the previous step. Make a note of the DN and password; you will need this information to complete the LDAP setup.
5. Enable LDAP on the Directory tab in the administration window.
6. Migrate configuration information to the LDAP directory server (optional).

Installing the schema extensions

The Host On-Demand extensions to the LDAP directory schema are provided in several files that are located in the LDAP subdirectory of the publish directory (for example, `C:\hostondemand\HOD\ldap)` . These files contain extensions to the LDAP schema and are stored in the standard slapd format. The schema extensions must be in effect before Host On-Demand can store configuration information in an LDAP server. Contact your LDAP administrator to have these schema extensions installed.

Your LDAP administrator may have already installed these schema extensions for use by another IBM product. If so, skip these steps. If you are using the IBM SecureWay Directory Server Version 3.1.1 or 3.2.1, the schema is pre-installed, so you can skip these steps also.

To install the Host On-Demand schema extensions on a Netscape LDAP Directory server:

1. Copy the following slapd files to the LDAP server:

   ```
   Netscape.IBM.at
   Netscape.IBM.oc
   ```

2. Stop the LDAP server.
3. Edit the `slapd.conf` file and add the following statements:

   ```
   userat "<Netscape LDAP config directory>/Netscape.IBM.at"
   useroc "<Netscape LDAP config directory>/Netscape.IBM.oc"
   ```

4. Restart the LDAP Server.

To install the Host On-Demand schema extensions on an IBM LDAP Directory server:

1. Copy the following slapd files to your LDAP server:

   ```
   V2.1.IBM.at
   V2.1.IBM.oc
   ```

2. Stop the LDAP server.
3. Edit the `slapd.at.conf` file and add the following statement to the end of the file:

   ```
   include /etc/V2.1.IBM.at
   ```

4. Edit the `slapd.oc.conf` file and add the following statement to the end of the file:

   ```
   include /etc/V2.1.IBM.oc
   ```

5. Restart the LDAP server.

Configuring LDAP support

The default operational mode for Host On-Demand is to use the private data store. Using an LDAP directory server to manage and share your definitions across multiple Host On-Demand servers is an option that must be carefully planned and executed. Before you switch your Host On-Demand server over to using the LDAP directory server, refer to implications of migrating to LDAP in the Host On-Demand online help.

1. Open the Administration window and logon to Host On-Demand.
2. Click Services > Directory Service
3. Click the Use Directory Service (LDAP) box and then enter the LDAP server information.

   Destination Address
   Type the IP address of the LDAP directory. Use either the host name or dotted decimal format. The default is the host name of the Host On-Demand server.

   Destination Port
   Type the TCP/IP port on which the LDAP server will accept a connection from an LDAP client. The default port is 389.

   Administrator Distinguished Name
   Type the distinguished name (DN) of the directory administrator that allows Host On-Demand to update information. You must use the LDAP string representation for distinguished names (for example, `cn=Chris Smith,o=IBM,c=US`).

   Administrator Password
   Type the directory administrator's password.

Distinguished Name Suffix

Type the distinguished name (DN) of the highest entry in the directory information tree (DIT) for which information will be saved. Host On-Demand will store all of its configuration information below this suffix in the DIT. You must use the LDAP string representation for distinguished names (for example, `cn=HOD,o=IBM,c=US`).

Migrate Configuration to Directory Service

To migrate users and groups from the private data store to the LDAP directory, click the check box. Migrating to LDAP has significant implications for your group and user configuration information. Refer to LDAP Migration Implications in the online help for more information. You can check this box either when you switch to the directory server, or after you have made the switch.

The Redirector configuration is not migrated to the directory server.

Note: If you have a problem connecting to LDAP and migrating, try to connect to LDAP first. Then, after successfully connecting, try to migrate.

4. Click Apply.

   When you are asked to authenticate with the LDAP directory for the first time, specify a user ID of ″admin″ and a password of ″password″. You can change this password after the first log on. Even though you might have changed your password for the private data store, that ID and password continues to be valid for the private data store only. For the LDAP directory, a separate user ID and password are required. To avoid confusion, you can change your LDAP directory password to be the same as your private data store password.

Changes made on this panel are effective immediately. Once you have switched to the LDAP server, subsequent user-related changes will be made only on the LDAP server, including administrative changes to groups, users, or sessions, and changes such as new passwords, macros, keyboard changes, etc., by either the administrator or a user.

Chapter 11. Database On-Demand overview

Note: If you are using Database On-Demand with Netscape 4.x, you must turn the Just In Time (JIT) compiler off. Unfortunately, due to problems found with the JIT compiler, this means that you cannot take advantage of both the Database On-Demand and integrated Windows domain logon functions.

Database On-Demand is a Java applet that allows users to perform SQL requests to iSeries databases through a JDBC driver. Database On-Demand is shipped with a JDBC driver for the iSeries. Other user-installed JDBC drivers can be registered and used, although IBM does not provide support for these drivers.

Features of Database On-Demand include:

- A graphical interface to aid in constructing SQL statements and File Upload statements
- The ability to display on screen the results of the executable statements you build, to save the results of SQL statements in various file formats and to upload entire files in various formats to a host database
- The ability to create dynamic queries, using the graphical interface, that can be executed or saved for later use

For more Database On-Demand overview information, see Database On-Demand in the Host On-Demand online help.

To configure users so they can access Database On-Demand, you must first either have groups and users defined or define them. Then you can define the database functions that groups and users can perform and later manage the statements that users have created. The administrator cannot create SQL statements for users.

For more detailed information about setting up groups and users to access Database On-Demand, see getting started with Database On-Demand and setting Database On-Demand options for users in the Host On-Demand online help.

If you wish to use multiple code pages with Database On-Demand, you must add jar or cab files to your HTML. Only those code pages that correspond to the language of the HTML file are automatically loaded, so for example you are running from a French computer but you want to access a Dutch host, you must make these modifications.

If you are using Database On-Demand as a Download Client with Netscape 6 or another Java2-enabled browser, then the HODDatabase_xx.html file must be modified, where xx is the two- or four-letter country or region designator. Look for the line that starts with the ″APPLET archive=″ tag. Add the correct jar filename from the table below.

If you are using Database On-Demand as a Cached Client with a non-Java 2 enabled browser (such as Internet Explorer 5.x), then you must edit the file HODDatabaseCached_xx.html. In the line starting ″PARAM NAME=PreloadComponentList″, add the correct component from the table below.

If you are using Database On-Demand as a Cached Client with Netscape 6 or another Java2-enabled browser, then you must make two changes to the

HODDatabase_J2_xx.html file. For the first change, look for the line that begins PARAM NAME=″cache_archive″. In the list of jar files which follows, add the jar filename from the table below. For the second change, look for the line which begins with ″document.writeln″. This line will contain a number of instances of the string ″HODVersion + ′,′″ . This list indicates to the JRE 1.3 the versions of each of the jar files. Thus, if a jar file is added to the list of cache archives, an additional cache_version must be specified. So, for every jar file which is added to the cache_archive, add another instance of the string ″HODVersion + ′,′″ . As an example, assume that we start with the French version of Database On-Demand, and we want to be able to also access a host with Dutch code pages.

For the Download Client running on a Java2-enabled browser, in the file HODDatabase_fr.html, the line:

```
<APPLET archive="ha_fr.jar,hoddba.jar,hodsql.jar"
 CODE="com.ibm.eNetwork.dba.dba.class" WIDTH=584 HEIGHT=450>
```

becomes:

```
<APPLET archive="hacp1b.jar,ha_fr.jar,hoddba.jar,hodsql.jar"
 CODE="com.ibm.eNetwork.dba.dba.class" WIDTH=584 HEIGHT=450>
```

For the Cached Client on a non-Java 2 enabled browser, in the file HODDatabaseCached_fr.html, the line:

```
<param name=PreloadComponentList value=HABASE;HODBASE;HODDBAS;HODSQL;HATRACE;HODCFG>
```

becomes:

```
<param name=PreloadComponentList value=HACP1B;HABASE;HODBASE;HODDBAS;HODSQL;HATRACE;HODCFG>
```

For the Cached Client on a Java2-enabled browser, we will change the file HODDatabase_J2_fr.html, the two lines:

```
<PARAM NAME="cache_archive" VALUE="ha_fr.jar,hoddba.jar,hodsql.jar,hodimg.jar">
document.writeln('<PARAM NAME="cache_version" VALUE="' +
HODVersion + ',' + HODVersion',' + HODVersion + ',' +
HODVersion + ',' + HODVersion + '">');
```

become:

```
<PARAM NAME="cache_archive" VALUE="ha_fr.jar,hoddba.jar,hacp1b.jar">
document.writeln('<ARAM NAME="cache_version" VALUE="' +
HODVersion + ',' + HODVersion',' + HODVersion + ',' +
HODVersion + ',' + HODVersion + '">');
```

Note: The total number of occurrences of the HODVersion string must be the same as the number of .jar files specified in the cache_archive parameter.

The following table lists the supported code-page languages, the corresponding .jar file names, and the cached component names:

Code-page language	.JAR file name	Cached component
Arabic	hacpar.jar	HACPAR
Czech, Hungarian, Polish, Slovenian	hacpce.jar	HACPCE
Danish, Finnish, Dutch, Norwegian, Swedish	hacp1b.jar	HACP1B

German, Spanish, French, Italian, Portuguese, Brazilian Portuguese	hacp1a.jar	HACP1A
Greek	hacpgr.jar	HACPGR
Hebrew	hacphe.jar	HACPHE
Japanese	hacpja.jar	HACPJA
Korean	hacpko.jar	HACPKO
Russian	hacpru.jar	HACPRU
Simplified Chinese	hacpzh.jar	HACPZH
Thai	hacpth.jar	HACPTH
Turkish	hacptr.jar	HACPTR
Traditional Chinese	hacptw.jar	HACPTW

Chapter 12. National language support

Host On-Demand is provided in many languages. The session windows, configuration panels, help files, and the documentation have been translated. In addition, display, keyboard, and processing support is provided for Arabic, Hebrew, Thai, and Hindi. This support is fully explained in the help.

All the translated versions are provided on the CDs and on the zSeries tapes. When you install Host On-Demand on Windows platforms or AIX using the graphical installation program, you can choose which languages to install. On the other operating systems, all the languages are always installed. Arabic, Hebrew, Thai, and Hindi support is always installed on all operating systems.

National language support is operating-system dependent, so the appropriate font and keyboard support for the language you want to use must be installed in the operating system. For example, if you want to use French as the host-session language but do not have the French font and keyboard support installed, you may not be able to display the correct characters.

Note: DBCS cannot be used as the HTML file name.

Supported languages

The languages into which Host On-Demand has been translated are listed below, along with the language suffixes you can use to load translated versions of the Host On-Demand clients.

Language	Language suffix
Simplified Chinese	zh
Traditional Chinese	zh_TW
Czech	cs
Danish	da
Dutch	nl
English	en
Finnish	fi
French	fr
German	de
Greek	el
Hungarian	hu
Italian	it
Japanese	ja
Korean	ko
Norwegian	no
Polish	pl
Brazilian Portuguese	pt
Portuguese	pt_PT

Russian	ru
Slovenian	sl
Spanish	es
Swedish	sv
Turkish	tr

Supported host code pages

Host On-Demand supports multiple code pages. You can specify these code pages on a session-by-session basis.

3270 and 5250 code pages

The code pages specified below are supported by the 3270 and 5250 emulators. You can select them in the Session Configuration window.

Country or region	Code page	Note
Arabic Speaking	420	
Austria	273	
Austria (Euro)	1141	
Belarus	1025	
Belarus (Euro)	1154	
Belgium	037	
Belgium (Euro)	1140	
Belgium (Old Code)	274	
Bosnia/Herzegovina	870	
Bosnia/Herzegovina (Euro)	1153	
Brazil	037	
Brazil (Euro)	1140	
Brazil (Old)	275	
Bulgaria	1025	
Bulgaria (Euro)	1154	
Canada	037	
Canada (Euro)	1140	
China (Simplified Chinese Extended)	1388	
Croatia	870	
Croatia (Euro)	1153	
Czech Republic	870	
Czech Republic (Euro)	1153	
Denmark	277	
Denmark (Euro)	1142	
Estonia	1122	
Estonia (Euro)	1157	
Finland	278	

Finland (Euro)	1143	
France	297	
France (Euro)	1147	
FYR Macedonia	1025	
FYR Macedonia (Euro)	1154	
Germany	273	
Germany (Euro)	1141	
Greece	875	
Hebrew (New Code)	424	
Hebrew (Old Code)	803	
Hindi	1137	5250 display only
Hungary	870	
Hungary (Euro)	1153	
Iceland	871	
Iceland (Euro)	1149	
Italy	280	
Italy (Euro)	1144	
Japan (Katakana Extended)	930	
Japan (Katakana Unicode Extended)	1390	3270 only
Japan (Katakana)	930	
Japan (Latin Extended)	939	
Japan (Latin Unicode Extended)	1399	
Korea (Euro)	1364	
Korea (Extended)	933	
Latin America	284	
Latin America (Euro)	1145	
Latvia	1112	
Latvia (Euro)	1156	
Lithuania	1112	
Lithuania (Euro)	1156	
Multilingual	500	
Multilingual ISO (Euro)	924	
Multilingual (Euro)	1148	
Netherlands	037	
Netherlands (Euro)	1140	
Norway	277	
Norway (Euro)	1142	
Open Edition	1047	
Poland	870	
Poland (Euro)	1153	

Portugal	037	
Portugal (Euro)	1140	
Romania	870	
Romania (Euro)	1153	
Russia	1025	
Russia (Euro)	1154	
Serbia/Montenegro (Cyrillic)	1025	
Serbia/Montenegro (Cyrillic; Euro)	1154	
Slovakia	870	
Slovakia (Euro)	1153	
Slovenia	870	
Slovenia (Euro)	1153	
Spain	284	
Spain (Euro)	1145	
Sweden	278	
Sweden (Euro)	1143	
Taiwan (Traditional Chinese Extended)	937	
Taiwan (Traditional Chinese Extended; Euro)	1371	
Thai	838	
Thai (Euro)	1160	
Turkey	1026	
Turkey (Euro)	1155	
Ukraine	1123	
Ukraine (Euro)	1158	
United Kingdom	285	
United Kingdom (Euro)	1146	
United States	037	
United States (Euro)	1140	

Notes:

- 3270 host print with a Printer Definition Table (PDT) supports only Latin-1, DBCS, bidirectional, and Thai code pages. Other code pages are supported only on Windows platforms without a PDT.
- In order to include more characters (which are defined in the GB18030 standard by the Government of the People's Republic of China), 6582 Unicode Extension-A and 1,948 additional non-Han characters (Mongolian, Uygur, Tibetan, and Yi) were added to the Simplified Chinese code page 1388 for Host On-Demand Version 6.

VT code pages

Language	Code page

Arabic	ASMO 708 and ASMO 449
British	1101
DEC Greek	
DEC Hebrew	
DEC Multinational Replacement Character Set	1100
DEC Technical	
Dutch	1102
Finnish	1103
French	1104
French Canadian	1020
German	1011
Hebrew NRCS	
ISO Greek Supplemental (ISO Latin-7)	813
ISO Hebrew Supplemental	
ISO Latin-1	819
Italian	1012
Norwegian/Danish	1105
PC Danish/Norwegian	865
PC International	437
PC Multilingual	850
PC Portugese	860
PC Spanish	220
Spanish	1023
Swedish	1106
Swiss	1021
United States	1100

CICS Gateway code pages

Code page	Character set
000	Auto-Detect (default)
437	Latin-1
813	ISO Greek (8859_7)
819	ISO Latin 1 (8859_1)
850	Latin 1
852	Latin 2
855	Cyrillic
856	Hebrew
857	Latin 5
864	Arabic
866	Cyrillic

869	Greek
912	ISO Latin 2 (8859_2)
915	ISO Cyrillic (8859_5)
920	ISO Latin 5 (8859_9)

User-defined character mapping

For double-byte character set (DBCS) languages, you can use customized user-defined character (UDC) mapping in your session (3270, 5250, 3270 host print) instead default mapping. You can create a UDC translation table using the UDC mapping editor to store customized mapping for your session. For instructions for how to use the UDC mapping editor to change your character mapping, refer to the online help.

Appendix A. Locally installed clients

The locally installed client installs to a local disk. The client applet is loaded directly into the default system browser, so there is no download from a server. The most common reason to configure a local client is for users who connect remotely over slow telephone lines, where download time can be an issue and connectivity is unpredictable. You can also use the locally installed client to test host access capabilities without installing the full Host On-Demand product.

Operating systems that support the locally installed client

Host On-Demand can be installed as a client on the following operating systems:

- Windows 95
- Windows 98
- Windows Millennium (Me)
- Windows NT 4.0 with SP3 or later
- Windows 2000

The locally-installed client requires 155MB of disk space.

Installing Host On-Demand as a client

To install Host On-Demand on a Windows NT or 2000 workstation, you must be a member of the Administrators group.

1. Insert the CD and run `setup.exe lc` from the `\win32` directory of the CD.
2. Click Install.
3. Choose a Typical or Custom installation.
   - Typical installs the Host On-Demand Java applets and the information library in English and the native language of your workstation.
   - Custom allows you to choose components to install: Host On-Demand Java applets, the information library and the Host Access Class Library. In addition to English, you can also select any of the other supported languages.
4. Proceed through the rest of the windows.
5. If you have not already done so, read the readme available in the last window.

At the end of installation, the Host On-Demand Service Manager is configured and started automatically. On Windows NT and 2000, the Service Manager is installed as a Service; on Windows 95, Windows 98 and Windows Millennium (Me) it is added to the Startup folder.

Starting the client

To start Host On-Demand as a client, click Start > Programs > IBM Host On-Demand > Host On-Demand.

Removing the client

1. Stop the Host On-Demand Service Manager:
   a. Press `Ctrl+Alt+Del` once to open the Close Program window.
   b. Highlight the JRE task, then click End Task.
2. Use Add/Remove Programs from Control Panel. If InstallShield does not remove the `hostondemand` directory, you must remove it manually.

Appendix B. Manually installing SSL security capability on AIX

If you intend to use an AIX server to support secure connections from clients, you must install additional files.

Before installing the AIX server security files over an existing installation, remove all lib*.so files from the hostondemand/bin directory.

Note: If you are running AIX 4.2, you must first upgrade to AIX 4.3, uninstall the previous version of Host On-Demand, and install Host On-Demand Version 6 using the hod60srv.AIX43.SSL.tar file.

You must also install JDK 1.1.8 or 1.3.

The following steps assume you are using the default server and publish directories. To install the security files:

1. Enter the following commands to unpack the main file:

   ```
   cd /usr/opt/hostondemand
   tar -xf /cdrom/tar/HOD60AIX.tar
   ```

2. The file extracted from HOD60AIX.tar is hod60srv.AIX43.SSL.tar. This file contains security files to be added to the server directory of an AIX 4.3 installation.
3. To add the extra files to the installation, untar the hod60srv.AIX43.SSL.tar file to the server directory. Enter the following commands:

   ```
   cd /usr/opt/server_directory
   rm bin/lib*.so
   tar -xf ./hod60srv.AIX43.SSL.tar
   ```

4. The GSK security library must also be installed. To extract the installp images, enter the following commands:

   ```
   cd /cdrom/tar/
   ```

   From the current directory, type `smit` to start the System Management Interface Tool (SMIT):

   a. From the System Management screen, click Software Installation and Maintenance.
   b. Click Install and Update Software.
   c. Click Install and Update from ALL Available Software.
   d. Type `./` when asked for INPUT device/directory, then click OK.
   e. Click List in the SOFTWARE to install field.
   f. In the list of software to install, highlight the line labeled gskkm, then click OK.
   g. Click OK on the Install and Update From ALL Available Software window.
   h. Click OK to close the confirmation message and install the software.

Before it starts, the Certificate Management program copies the English version of its help files to the hostondemand/bin directory. This is done by the following line in the file hostondemand/bin/CertificateManagement:

```
cp en/HODServerKMHelp.class
```

If you want to have access to the help for a different language, you must change the directory from which the HODServerKMHelp.class file is copied. For example, if you want to use the Spanish help files, change the above line to:

```
cp es/HODServerKMHelp.class
```

Appendix C. Configuring on iSeries

Configuring iSeries servers for secure connection

The iSeries severs can be configured to use certificates from a public signing agency or from a private certificate management system, like the AS/400 Digital Certificate Manager. Before you enable SSL, decide which type of certificate to use. See Deciding where to obtain your digital certificates on the iSeries Web site.

You must have the following programs installed to use SSL with iSeries:

- Digital Certificate Manager (DCM), option 34 of OS/400
- TCP/IP Connectivity Utilities for AS/400
- IBM HTTP Server for AS/400
- One of the IBM Cryptographic Access Provider products: 40-bit, 56-bit, or 128-bit. The bit size for these products indicates the varying sizes of the digital keys that they employ. A higher bit size results in a more secure connection. Some of these products are not available in all areas due to government export regulations.

Configuring a Telnet server for secure connection

The following table describes the steps to enable Telnet with SSL. You will need to repeat this step for each iSeries that you wish to use secure connections with.

OS/400 level	Web page
Version 5 Release 1	Secure Telnet on the iSeries Web site. Perform Step 1 only. Client authentication is discussed in a section below.
Version 4 Release 4 and Version 4 Release 5	Telnet server and SSL on the AS/400 Web site
Version 4 Release 2 and Version 4 Release 3	Telnet SSL Proxy Server on the AS/400 Web site

Configuring the Host On-Demand Telnet keyring

1. Type the following command: `qsh`
2. Change to the Host On-Demand lib directory: `cd /qibm/proddata/hostondemand/hod`
3. Obtain a server certificate from an SSL-enabled Telnet server. Remember to substitute the value for host.name with the TCP/IP host name or dotted address in the string listed below. 992 is the commonly used port for secure connections. This command may span two lines but should be entered as one line:

   ```
   java -classpath .:/QIBM/ProdData/hostondemand/lib/sm.zip com.ibm.hodsslight.tools.keyrng
   CustomizedCAs connect host.name:992
   ```

   This command may take a few minutes to complete. If you are prompted for a password, press Enter. If this is the first certificate, a new CustomizedCAs object is created. Select the number of the Certificate Authority (CA) certificate that you want to add to the Host On-Demand Telnet keyring. Be sure to add

the CA certificate and not the site certificate. If the port is not responding, refer to Configuring iSeries servers for secure connection. Repeat Step 3 for each Telnet server.

4. To view the contents of the keyring, type the following (this command may span two lines but should be entered as one line):

```
java -classpath .:/QIBM/ProdData/hostondemand/lib/sm.zip com.ibm.hodsslight.tools.keyrng
CustomizedCAs verify
```

5. Press F3 to exit qsh.

If you have multiple iSeries machines and would like to create a single certificate that all the machines can use, consider cross certification. Refer to iSeries Wired Security: Protecting Data over the Network, OS/400 Version 5 Release 1DCM and Cryptographic Enhancements (SG24-6168) for additional information about cross certification.

Client authentication

For additional security, consider SSL with client authentication to tightly control who can Telnet to your system over the Internet. For example, you can configure the Telnet server to only allow authentication if the client certificate was issued by your iSeries (through Digital Certificate Manager).

The client certificates have a limited validity period (for example, 90 days). When the certificate expires, the user must perform the Client Certificate Download process in order to continue. This process requires a valid iSeries user ID and password.

Not all Telnet client software is capable of client authentication. When enabled, all SSL-enabled Telnet connections to the iSeries require a user certificate.

OS/400 level	Detailed instructions
Version 5 Release 1	Secure Telnet on the iSeries Web site.
Version 4 Release 4 and Version 4 Release 5	Telnet Server; SSL Client Authentication on the TCP/IP for OS/400 Web site

Configuring the Host On-Demand OS/400 proxy for secure connections

The OS/400 proxy can be configured to encrypt file transfer and Database On-Demand connections. To do this, the following additional software must be installed on each target iSeries:

- IBM Cryptographic Access Provider
- IBM Client Encryption
- Host Servers
- Digital Certificate Manager

1. You should control authorization of the users to the files. To help you to meet the SSL legal responsibilities, you must change the authority of the directory that contains the SSL files to control user access to the files. In order to change the authority, do the following:
   a. Enter the command `wrklnk '/QIBM/ProdData/HTTP/Public/jt400/*'`
   b. Select option 9 in the directory (SSL40, SSL56, or SSL128).
      1) Ensure *PUBLIC has *EXCLUDE authority.

2) Give users who need access to the SSL files *RX authority to the directory. You can authorize individual users or groups of users. Remember that users with *ALLOBJ special authority cannot be denied access to the SSL files.

2. From a web browser, access http://<server.name>:2001 (where <server.name> is the TCP/IP host name of your iSeries). If you are unable to connect, start the HTTP server with the following OS/400 command:

   ```
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
   ```

3. Enter the OS/400 user profile and password (when prompted). You must have *ALLOBJ authority to complete the configuration activities below.
4. Click on **Digital Certificate Manager**.
5. Click on **System Certificates**.
6. Click **Work with Secure Applications**.
7. Click **QIBM_OS400_QZBS_SVR_CENTRAL**, then click **Work with System Certificate**.
8. Verify that the *DFTSVR certificate is selected and click **Assign New Certificate**.
9. Repeat steps 7 and 8 for the following applications:
   - QIBM_OS400_QZBS_SVR_DATABASE
   - QIBM_OS400_QZBS_SVR_DTAQ
   - QIBM_OS400_QZBS_SVR_NETPRT
   - QIBM_OS400_QZBS_SVR_RMTCMD
   - QIBM_OS400_QZBS_SVR_SIGNON
   - QIBM_OS400_QZBS_SVR_FILE
   - QIBM_OS400_QRW_SVR_DDM_DRDA
10. Type the following OS/400 command: `QSH`
11. Type the following command:

    ```
    cd /qibm/proddata/hostondemand/lib
    ```

    Note: cd must be in lower case
12. The following command obtains a server certificate from an SSL-enabled Telnet server. This command may span three lines.

    ```
    java -classpath .:/QIBM/ProdData/hostondemand/lib/sm.zip
    com.ibm.hodsslight.tools.keyrng com.ibm.as400.access.KeyRing connect
    host.name:9476
    ```

    Notes:

    a. Substitute the value `host.name` with the TCP/IP host name or dotted address in the string listed below. The value 9476 is the commonly used port for secure connections.

    b. The 9476 port is usually the secure signon server port

    Proceed as follows for this command:

    a. You must enter `toolbox` as the password. Press Enter to continue.

    b. Multiple pages of information may be displayed; press the Page Up and Page Down keys to see additional details about the certificates, including the fingerprint. You will typically have two selections to choose from:

       0 Trust the Telnet server

       1 Trust the Certificate Authority

    c. Select 0 to trust the Telnet server certificate, then press Enter.

Repeat the above steps for each target iSeries server.

Secure Web serving

The Host On-Demand server uses the Web server to download program objects to the browser. This information can be encrypted, but with a considerable performance impact. Refer to the redbook AS/400 HTTP Server Performance and Capacity Planning (SG24-5645) for more information.

The default port for secure web serving is 443. If that port is not enabled, port 80 is used. To enable secure web serving, perform the following steps:

1. From a Web browser, enter: `http://<server.name>:2001` (where <server.name> is the TCP/IP host name of your iSeries). If you are unable to connect, start the HTTP server with the following OS/400 command:

   ```
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
   ```

2. Enter the OS/400 user profile and password (when prompted). You must have *ALLOBJ and *SECADM authorities to complete the remaining configuration activities.
3. Click on **IBM HTTP Server for AS/400**.
4. Click on **Configuration and Administration**.
5. Click on **Configurations**.
6. Choose the **CONFIG** configuration from the list.
7. Click on **Security Configuration**.
8. For the **Allow HTTP connections** and **Allow SSL connections** selections:
   - Port number (443)
   - Select SSL Client authentication **None**.
   - Select **Apply**.
9. Click on the **AS/400 Tasks** button on the lower left side of the screen.
10. Click on **Digital Certificate Manager**.
11. Click on **System Certificates**.
12. Click **Work with Secure Applications**.
13. Click **QIBM_HTTP_SERVER_CONFIG**; then click **Work with System Certificate**.
14. Click **Assign New Certificate**.
15. End the administration HTTP server instance with the following OS/400 command:

    ```
    ENDTCPSVR SERVER(*HTTP) HTTPSVR(DEFAULT)
    ```

16. Wait 10 seconds for the HTTP instance to shutdown.
17. Start the administration HTTP server instance with the following OS/400 command:

    ```
    STRTCPSVR SERVER(*HTTP) HTTPSVR(DEFAULT)
    ```

18. From a Web browser, enter `https://<server.name>/hod/hodmain.html` (where <server.name> is the TCP/IP host name of your iSeries).

Table 1. Additional iSeries-related web pages

Title	Title Web page
Common SSL problems	Troubleshooting SSL-enabled Telnet server
Telnet exits—filter Telnet service by IP address	Welcome to TCP/IP reference information

Table 1. Additional iSeries-related web pages (continued)

Title	Title Web page
National language exit	Download Telnet exit program files

Installing the iSeries Toolbox for Java

The iSeries Toolbox for Java is a set of Java classes that enable you to write client/server applications and applets that work with data residing on your iSeries. You can also run such applications on the OS/400 Java Virtual Machine (JVM).

The Toolbox uses iSeries servers as access points to the system. Each server runs as a separate job on the iSeries, and each job sends and receives datastreams on a socket connection.

The access classes provide low-level access to the following iSeries resources:

- Databases via a JDBC driver or record-level access
- Integrated File System
- Programs
- Commands
- Data queues
- Print
- Digital certificates
- Jobs
- Message queues
- Users and groups
- User spaces

Graphical programming interfaces are available for:

- Databases (both JDBC and record-level access)
- Command call
- Data queues
- Integrated
- File system
- Jobs
- Message queues
- Print
- Program call
- Users and groups

The following files are located on the Host Access Toolkit CD, **not** the OS/400 CD:

- `jt400_all.zip` contains `jt400.zip`, `jt400.jar`, utilities files, and help and message files
- `jt400_doc_en.zip` contains the Programmer's Guide in English
- `jt400_doc_ja.zip` contains the Programmer's Guide in Japanese
- `jt400_doc_ko.zip` contains the Programmer's Guide in Korean
- `jt400_doc_zh.zip` contains the Programmer's Guide in Simplified Chinese (PRC)
- `jt400_doc_es.zip` contains the Programmer's Guide in Spanish

- `jt400_doc_zh_TW.zip` contains the Programmer's Guide in Traditional Chinese.

To install the iSeries Toolbox for Java on your workstation, unzip the appropriate files. For example, if you want to install the code and the English version of the Programmers Guide, `unzip jt400_all.zip and jt400_doc_en.zip` .

You must use a utility that supports long filenames.

For additional information on the toolbox, see `http://www.as400.ibm.com/toolbox`.

Appendix D. Netscape 6.0 and Java2-enabled Web browser issues

Host On-Demand Version 6 clients are supported on Java2-enabled Web browsers, such as Netscape 6.0, Netscape 6.01, Mozilla 0.9.0, and the IBM Web Browser for OS/2. These Web browsers use a Java2 Runtime Environment (JRE) plug-in that is supplied by Sun Microsystems Inc. or IBM. As newer versions are released, IBM will announce support on the Host On-Demand Web site. Older Web browsers, such as Microsoft Internet Explorer and Netscape 4.x on Windows, can also use the Java2 plug-in, but these browsers require converted HTML files to properly call the Java2 plug-in. Sun Microsystems Inc. provides an HTML converter. See `http://java.sun.com/products/plugin/1.3/docs/html_converter.html` for more information on this tool.

Limitations for Host On-Demand

Java2 has a stricter security model than older versions of Java. This imposes several restrictions on Host On-Demand:

- Function On-Demand client limitations: The Function On-Demand client will not work with Java2-enabled Web browsers.
- Host On-Demand Download client limitations: If you use HOD.html to load your download client, you will not be able to use the following functions:
  - 5250 - file transfer
  - Host print sessions
  - Import/export
  - SLP
  - License Use Management (LUM)
  - Thai sessions
  - FTP code-page converter
  - Bidirectional VT sessions
  - 5250 Hindi sessions

  There are three possible solutions to this problem:
  - Use the Host On-Demand Download client with Problem Determination. This client includes all of the Host On-Demand classes and is large.
  - Use the Host On-Demand cached client for Java2 browsers.
  - Use the Deployment Wizard to generate a set of custom HTML files.
- Cached client limitations: Host On-Demand administrators cannot stage the upgrade of their clients to Host On-Demand Version 6 using percent upgrade.
- Cached client removal limitations: Cached clients can no longer be removed with HODRemove.html. Users will need to use the Java Control Panel to clear the JRE cache. See Removing the cached client section below for more information.

Sun JRE limitations

Limitations with the Sun JRE Version 1.3x on Linux and Solaris functioning with getDocumentBase() cause most Host On-Demand clients not to work. Linux users can avoid the problem by using the IBM JRE. Solaris users that use Host On-Demand Version 6 and a Java2-enabled Web browser can avoid the problem by

using the Sun JRE Version 1.4 or by running a custom session1.html or session2.html file. You also see this limitation running the Sun plug-in with older browsers and converted HTML files. The IBM JRE for Windows 32-bit platforms and Linux can be downloaded free of charge from the IBM Web site. The OS/2 JRE is available on Software Choice.

The Sun JRE also has a limitation with Hindi character conversion. To avoid this problem, use the IBM JRE.

Run applet

Permission must be granted by the Java2 Policy Tool before user-defined applets will run; otherwise, the applet will silently fail.

Removing the cached client

The Host On-Demand Java files used to run the Host On-Demand cached client on a Java2-enabled Web browser are stored in the Java Runtime Environment (JRE) cache. The JRE cache can be cleared via the JRE Java Control Panel.

For the Sun JRE on Windows machines, the Java Control Panel can be started from the Windows Control Panel.

For the IBM JRE on a Windows machine, click Start - Programs - Java Control Panel.

For OS/2, run: `C:\java13\jre\bin\jctrlpnl.cmd`.

For Linux and the IBM JRE, run:

```
<JRE install directory>/jre/bin/JavaPluginControlPanel
```

(The install directory is normally /opt/IBMJava2-13)

For Linux and the Sun JRE, run:

```
<Java2 enabled web browser install directory>/plugins/java2/bin/ControlPanel
```

Once the Java plug-in Control Panel is started, click on the Cache tab on the top of the window, and then click on Clear JAR Cache. Clicking this button will clear the entire cache.

Cached client installation

The cached client installation from a CD or LAN drive is not possible. The JRE stores the .jar files in the cache according to their code base. The JRE considers the CD to be a different codebase; therefore, the JRE will still download the Host On-Demand client from the Web server.

Appendix E. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or region or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country or region where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

```
IBM Corporation
Department T01
Building B062
P.O. Box 12195
Research Triangle Park, NC 27709-2195
U.S.A.
```

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee. The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Appendix F. Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both: **IBM**

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation.

Other company, product, and service names may be trademarks or service marks of others.

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.